TRICARE Management Activity

Protected Health Information Management Tool (PHIMT)

Training Reference: User Admin Manual
Version 1.0

Prepared By:
Booz Allen Hamilton

This page lists all of the changes that have been made to the PHIMT User Admin Guide throughout its development.

Version	Release Date	Summary of Changes

I

TABLE OF CONTENTS

This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.

1.0 INTRODUCTION TO PHIMT

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires a covered entity, (i.e., the Military Health System (MHS)) to maintain a history of when and to whom disclosures of Protected Health Information (PHI) are made for purposes other than treatment, payment and healthcare operations (TPO). The MHS must be able to provide an accounting of those disclosures to an individual upon request. Authorizations and Restrictions from an individual to a covered entity are included in the information that is required for tracking purposes.

To comply with the requirements for disclosures, the TRICARE Management Activity (TMA) provides an electronic disclosure-tracking tool. The Protected Health Information Management Tool (PHIMT) stores information about all disclosures, authorizations, and restrictions that are made for a particular patient. PHIMT has a functionality built into it that can provide an accounting of disclosures, if necessary.

The Military Treatment Facility (MTF) should have knowledge of DoD 6025.18-R, Health Information Privacy Regulation. A MTF must provide an accounting of disclosures within 60 days of the request. If the covered entity cannot honor an accounting of disclosures within the 60-day period, it must provide information to the requestor as to the reason for the delay and expected completion date. The covered entity may extend the time to provide the accounting by no more than 30 days. Only one extension is permitted per request.

1.1 PHIMT Requirements

Before using PHIMT it is necessary to understand and ensure the operating requirements are met. PHIMT has specific requirements for the operating system, browser, and plug-ins.

1.1.1 System Requirements

Using PHIMT requires a Microsoft Windows application: Windows XP (home, professional); Windows 2000 (standard, professional, advanced); or Windows 98.

NOTE: *Windows NT does work with PHIMT in most cases, but some limitations may exist. Therefore, Windows NT is not supported for use with PHIMT.*

1.1.2 Browser Requirements

PHIMT requires the use of Microsoft Internet Explorer, version 6.0 or above.

NOTE: *Cookies and JavaScript should be enabled (these items are enabled in a default browser installation)*

1.1.3 Plug-Ins

PHIMT requires the use of Adobe Acrobat, version 6.0 or above. The application will also work with version 5.0 but the latest version is recommended.

NOTE: *To display the generated letters and reports in the browser, the Adobe Acrobat Plug-in is required. This is normally installed with Adobe Acrobat Reader. Download Adobe Acrobat for free at* *http://www.adobe.com*.

2.0 GETTING STARTED

In PHIMT, the User Admin is responsible for setting up all users within their facilities as directed by the MTF Privacy Officer. The HIPAA Support Center or another User Admin creates an account for the User Admin and provides them with their User Name and Password. The User Admin is responsible for establishing all the accounts for their MTF.

2.1 User Definitions And Roles

Each **User** is assigned to one or more organizations (an organization is a logical or physical entity such as an MTF, a Service or TMA).

- Within an organization, each user can have one or more roles.
- A user can have the same roles in multiple organizations, or different roles in multiple organizations.
- Roles are inherited through permission levels.

A **Role** is a named collection of permissions. Roles allow Users with the same permissions to be grouped under a unique name. PHIMT roles include: Regular User, User Admin, Privacy Specialist, and Tool Admin.

- A **Regular User** is a general role with basic functionality. This role can create disclosures and authorization requests that can be routed on to a Privacy Specialist.
- A **User Admin** is a local administrator for an MTF or a designated Service. This role allows one to add/modify users from within their Service and assigns roles. The email account administrators will handle this role for each MTF or Service.
- A **Privacy Specialist** is the Privacy Officer or designee at an MTF or Service level. This role allows the User to maintain disclosure reporting, approve/deny disclosure requests, amend requests, restrict and suspend disclosures, and to generate associated letters.
- A **Tool Administrator** has global access to the application and will be maintained by the HIPAA Support Center. This role allows the User to configure roles within MTFs, and create permissions within the application.

NOTE: Your particular user role will determine the PHIMT activities you are authorized to perform. For example, as a User Admin you can perform only those activities listed on the User and Admin tabs. Different user roles are authorized to access different tabs.

2.1.1 PHIMT Roles and Permissions

PHIMT roles and permissions are based on status-level relationships within service groups. These service groups consist of the Army, Navy, Air Force, and Coast Guard. Anyone in a given service group can be granted access to information required for them to perform their duties. Specific roles have corresponding permissions that determine who will have access to what. Individuals within PHIMT roles have access to information required for job performance as well as access to information accessible to those roles with fewer permissions. No individual will be granted access to information needed to perform duties that require a higher set of permissions. Those in roles with the highest levels of permissions will have access to all information within their service group. No individual within any service group will be granted access to information in a service group other than their own.

For example, TMA and Support, Group A the top tier, occupies those roles with the highest levels of permissions. These individuals are granted access to all information within their Service Group. Those individuals in the Service Groups who occupy roles requiring a lower level of permissions, Group B the second tier, do not have access to the information accessible to those in the top tier. However, Group B does have access to the information in tier C, comprised of roles requiring even lower permission levels. The third tier, Group C, is comprised of offices and command centers within the service groups. This tier can only access information necessary for them to complete their responsibilities. They do not have access to information within the higher tiers. There is absolutely no viewing of another's information outside of your own service group.

2.1.2 User Admin Role

In PHIMT, the User Admin is responsible for setting up all accounts for users within their facilities as directed by the MTF Privacy Officer. The User Admin creates and assigns user names and passwords, adds/modifies users from within their facility, assigns roles, and creates user-to-user relationships.

As a User Admin, it is your responsibility to verify the identity of individuals who access PHIMT. Verify the user's identity with a government issued photo ID and written request for PHIMT access signed by the Privacy Officer. The Chief Information Officer (CIO) may incorporate the requirement for a written request into an existing form used by the Information Office to grant access to other systems. You cannot create an account for those who cannot verify their ID or do not have the signature of approval by the Privacy Officer at that specific MTF.

When an individual no longer requires PHIMT access at the MTF, (ex., transfer, retirement), you must remove PHIMT access in compliance with the MTF policy.

2.1.3 Interaction with the Privacy Officer

In order for PHIMT to be most beneficial, users within departments that manage PHI, are assigned roles with a varying degree of permissions. Some of the departments that the Privacy Officer may wish to grant access include, (but are not limited to):

- Medical records
- Release of information
- Patient advocate
- Patient's rights
- Privacy office

Some or all individuals within the various departments may be designated as Regular Users or Privacy Specialists.

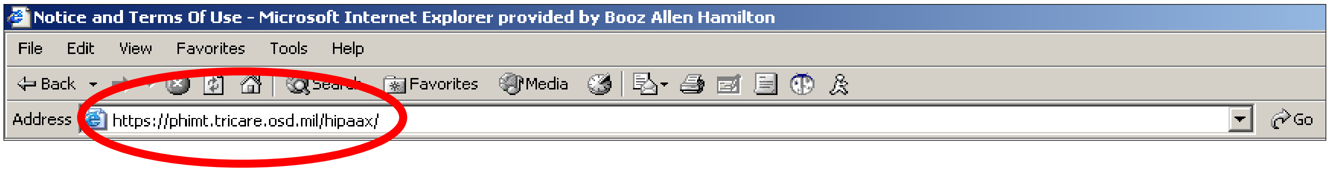
As a User Admin, you will create accounts and User-to-User Relationships as directed by the Privacy Officer. A collaborative effort is required to ensure the release of PHI is managed within PHIMT. Before establishing any accounts, the Privacy Officer will have an understanding of the way the MTF manages disclosures, the key individuals involved in the release of information and tracking of disclosures, and the approval process. A complimentary knowledge base will come from you and your understanding of how to create a workflow by routing the requests of a Regular User to a Privacy Specialist and from a Privacy Specialist to another Privacy Specialist, if necessary. Multiple User-to-User Relationships can be established throughout the facility.

3.0 ACCESSING AND USING PHIMT

Now that you have an understanding of why PHIMT was developed, are familiar with its capabilities and system requirements, and understand your role as a User Admin, you are ready to access the application.

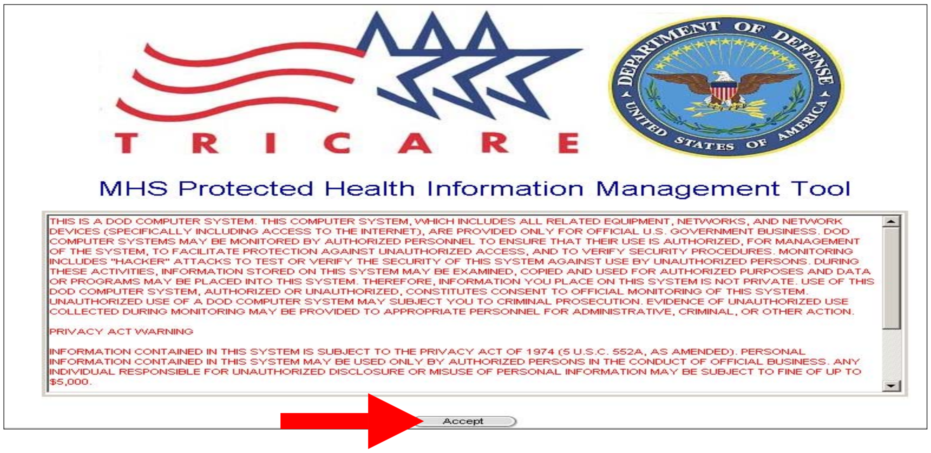
To login to the PHIMT application:

1. Enter the URL for PHIMT into the Web browser, https://phimt.tricare.osd.mil.


Notice and Terms Of Use - Microsoft Internet Explorer provided by Booz Allen Hamilton
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
https://phimt.tricare.osd.mil/hipaax/
Go

2. Read the Notice and Terms of Use.

3. Click on the **Accept** button.



THIS IS A DOD COMPUTER SYSTEM. THIS COMPUTER SYSTEM, WHICH INCLUDES ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING ACCESS TO THE INTERNET), ARE PROVIDED ONLY FOR OFFICIAL U.S. GOVERNMENT BUSINESS. DOD COMPUTER SYSTEMS MAY BE MONITORED BY AUTHORIZED PERSONNEL TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES. MONITORING INCLUDES "HACKER" ATTACKS TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM AGAINST USE BY UNAUTHORIZED PERSONS. DURING THESE ACTIVITIES, INFORMATION STORED ON THIS SYSTEM MAY BE EXAMINED, COPIED AND USED FOR AUTHORIZED PURPOSES AND DATA OR PROGRAMS MAY BE PLACED INTO THIS SYSTEM. THEREFORE, INFORMATION YOU PLACE ON THIS SYSTEM IS NOT PRIVATE. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO OFFICIAL MONITORING OF THIS SYSTEM. UNAUTHORIZED USE OF A DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE PROVIDED TO APPROPRIATE PERSONNEL FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ACTION.

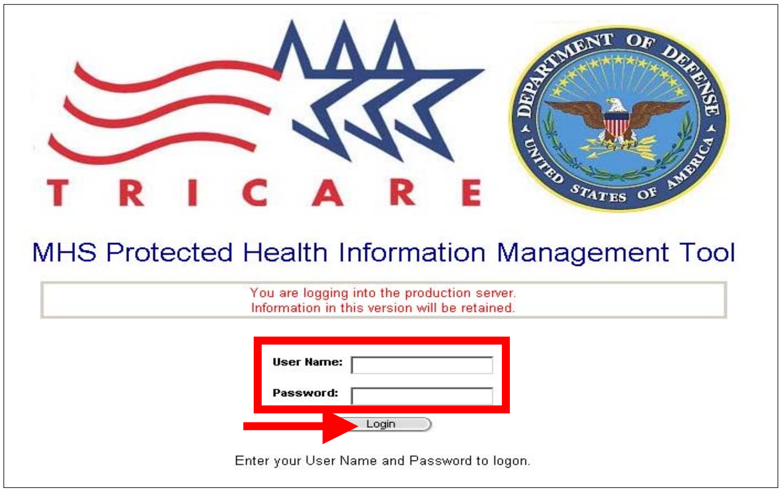
PRIVACY ACT WARNING

INFORMATION CONTAINED IN THIS SYSTEM IS SUBJECT TO THE PRIVACY ACT OF 1974 (5 U.S.C. 552A, AS AMENDED). PERSONAL INFORMATION CONTAINED IN THIS SYSTEM MAY BE USED ONLY BY AUTHORIZED PERSONS IN THE CONDUCT OF OFFICIAL BUSINESS. ANY INDIVIDUAL RESPONSIBLE FOR UNAUTHORIZED DISCLOSURE OR MISUSE OF PERSONAL INFORMATION MAY BE SUBJECT TO FINE OF UP TO $5,000.

- Log in using the User Name and temporary Password that has been assigned to you by the HIPAA Support Center.

4. Type in User Name and Password.

5. Click on the Login button.



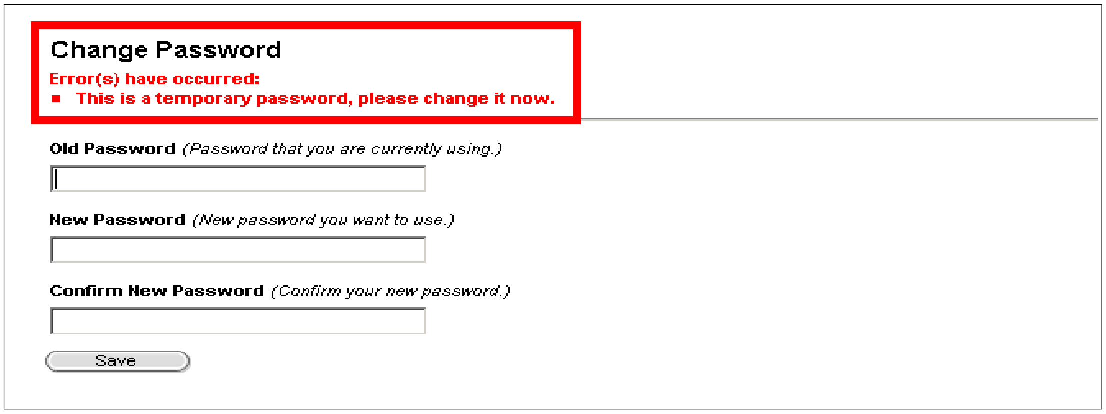
MHS Protected Health Information Management Tool

You are logging into the production server.
Information in this version will be retained.

Enter your User Name and Password to logon.

The first time you login you will be prompted to change your temporary password. Your new password must be 8 to 15 characters long and contain at least one of the following:

- Alphabetic uppercase character
- Alphabetical lower case character
- Arabic numeral (0,1,2,3,4)
- Non-alphanumeric special character (ex: !, @, #, $, etc.)



Change Password

Error(s) have occurred:

- This is a temporary password, please change it now.

Old Password (Password that you are currently using.)
New Password (New password you want to use.)
Confirm New Password (Confirm your new password.)
Save

4.0 USER ADMIN TABS

In PHIMT, the User Admin has access to two tabs:

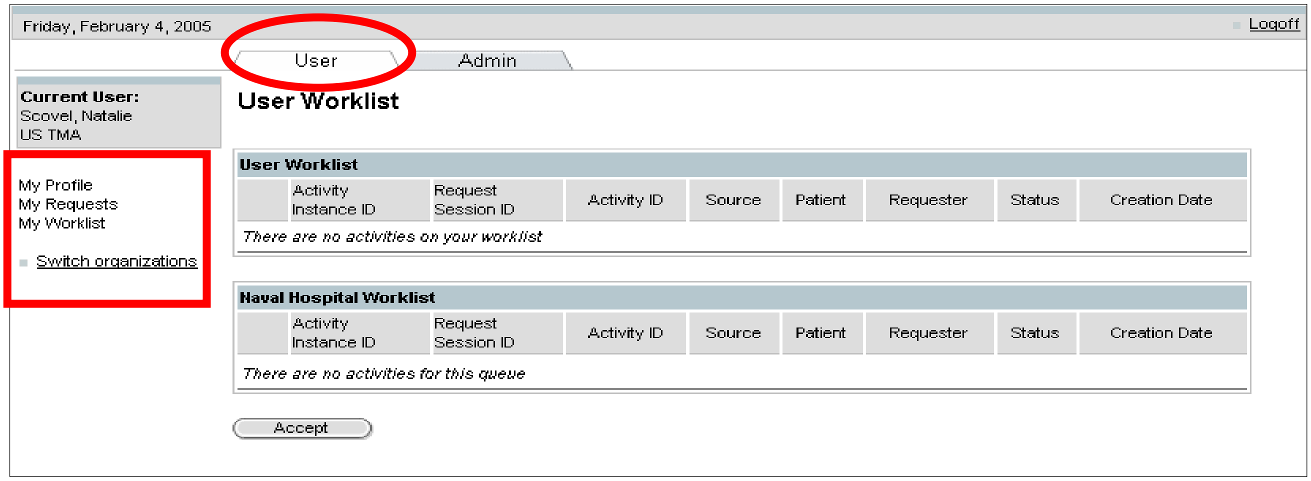
- User
- Admin

4.1 USER Tab

The **User** tab contains all PHIMT User related information.

As a User Admin role in PHIMT, you will have certain accesses in the User Tab by clicking on these hyperlinks:

- My Profile – update user information and create user-to-user relationships.
- My Requests – view the status of all requests you initiated.
- My Worklist – view and process all requests that have a task currently assigned to you
- Switch Organizations – switch the primary status of users, who are assigned to more than one organization, to a different organization.



Current User:
Scovel, Natalie
US TMA

User Worklist

User Worklist

	Activity Instance ID	Request Session ID	Activity ID	Source	Patient	Requester	Status	Creation Date
There are no activities on your worklist								

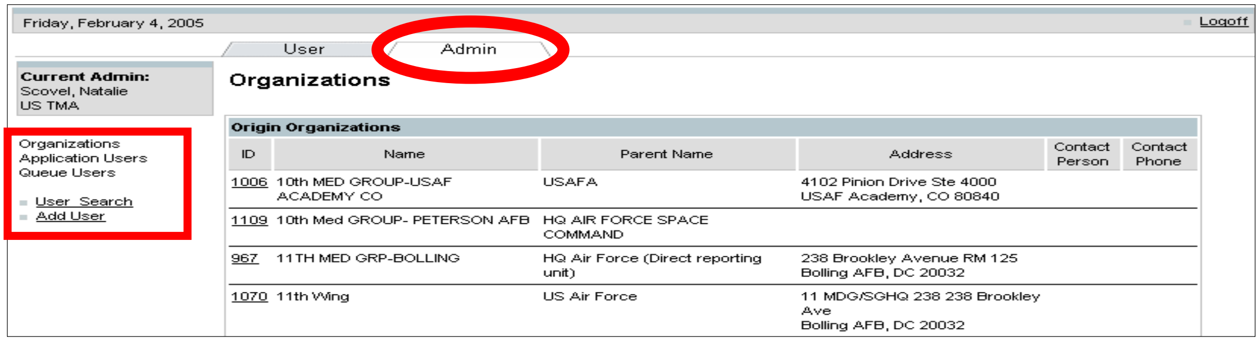
Naval Hospital Worklist

	Activity Instance ID	Request Session ID	Activity ID	Source	Patient	Requester	Status	Creation Date
There are no activities for this queue								

4.2 ADMIN Tab

Your role as a PHIMT User Admin, will provide you with certain accesses on the Admin tab by clicking on these hyperlinks:

- Organizations
- Application Users
- Queue Users
- User Search
- Add User



Current Admin:
Scovel, Natalie
US TMA

Organizations

Origin Organizations

ID	Name	Parent Name	Address	Contact Person	Contact Phone
1006	10th MED GROUP-USAF ACADEMY CO	USAFA	4102 Pinion Drive Ste 4000 USAF Academy, CO 80840		
1109	10th Med GROUP- PETERSON AFB	HQ AIR FORCE SPACE COMMAND			
967	11TH MED GRP-BOLLING	HQ Air Force (Direct reporting unit)	238 Brookley Avenue RM 125 Bolling AFB, DC 20032		
1070	11th Wing	US Air Force	11 MDG/SGHQ 238 238 Brookley Ave Bolling AFB, DC 20032		

5.0 UNDERSTANDING PHIMT SCREENS

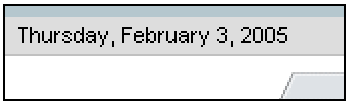
Each tab of the PHIMT screens contains some basic information that will be helpful to you when performing the various activities.

5.1 Screen Features

There are many features to the PHIMT screen that you can use to navigate your way through the many disclosure activities you will perform. These features are discussed here.

5.1.1 Date

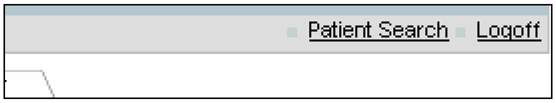
The date displays the current weekday, month, day, and year in the upper left corner of the PHIMT screen.



Thursday, February 3, 2005

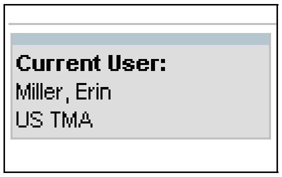
5.1.2 Navigational Options

Navigational options, such as patient search and logoff, provide directional hyperlinks that will help you to proceed through the PHIMT application. They are located in the upper right hand corner of the PHIMT screen.



5.1.3 Status Box

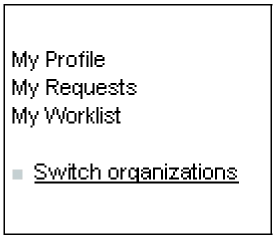
The gray status box shows current information and is located in the upper left hand corner of all PHIMT screens. The box displays the current user, user information such as organization and assigned role, patient information, and information about what disclosure activity is currently being performed. This information is updated when making inputs for various activities.



Current User:
Miller, Erin
US TMA

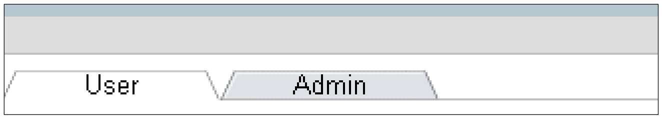
5.1.4 Activity Hyperlinks

The activity hyperlinks are located under the status box, on the left hand side of the PHIMT screen. This listing consists of hyperlinks for activities that can be performed while in a specific "tab." The hyperlinks may include: my worklist, patient profile, or authorization; depending on which tab you are using. Your user role will determine specific hyperlinks listed.



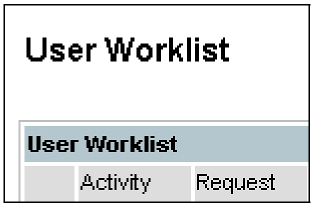
5.1.5 PHIMT Screen Tabs

PHIMT screen tabs are labels that are located at the top of the display screen. The tabs serve as file folders for different groupings of activities. The specific tabs will vary depending on what role you are assigned. User Admin tabs includes: User, Admin. Each tab allows for different activities.



5.1.6 Screen Title

The screen title is located directly under the tabs and above the display screen. This is the title of the particular screen being displayed (ex. user worklist, patient search results).



5.1.7 Display Screen/Application Window

The display screen/application window is the PHIMT users work area. These screens contain various fields in which to provide required information for proceeding through the PHIMT activities. To assist with data input, PHIMT provides text boxes, windows, calendar icons, and drop down menus. All features may not be on a particular user screen:

- *Radio buttons* – Radio buttons appear as black dots to indicate selection. You can toggle the buttons between selected and not selected.

- *Check marks* – Check marks are used to indicate a done or un-done status. You can toggle the marks between checked and unchecked.
- *Drop down menus* – Drop down menus provide the user with a list of possible selections from which to choose. Clicking on a particular selection causes it to be selected and appear in the "window." You can change a selection by clicking the arrow on the menu box and then clicking on a different item.
- *Text boxes* – Text boxes are empty fields in which you can provide information. At times, this data is requested as additional comments or for supplemental information.
- *Calendar icons* – Calendar icons are provided to make it easier for you to input required dates. Date inputs are specific dates chosen by you to clarify time limits on various PHIMT activities. Choose a date by selecting the arrow in the date window. A calendar icon appears for easy inputs. Click on the desired date or use the arrows near the month and year headings to display a date not currently shown. The date you select will appear in the date window.
- *Action buttons* – Action buttons are used to guide you through the PHIMT steps and processes. Click on these buttons to proceed through various activities. Examples of these buttons include: Next, Save, Create, and Update.

NOTE: These features will be discussed when they are used in an activity.

5.2 PHIMT Error Messages

PHIMT issues error messages when an entry or selection is not appropriate or complete. The message begins "Error(s) have occurred" and then follows with a bulleted list of the errors. For example, if you try to route an activity to someone who does not have access to that information, or you are not authorized to route the information to that particular person, PHIMT will display a message that indicating that you do not have the authority to perform that task. If you have not provided information for all the required data fields, PHIMT will issue a message indicating that information is missing. Once the error has been corrected, you can proceed to the next step in the PHIMT activity.

6.0 USER ADMIN ACTIVITIES

The following information will provide you with step-by-step instructions for adding users and assigning roles, editing user profiles, disabling user accounts, adding organizations, and establishing User-to-User Relationships (establishing office workflow).

Your role as User Admin requires you to perform various PHIMT activities establish and maintain user information. The steps for performing these activities will be presented here and include the following:

- Create user accounts
- Establish workflow
- Edit user profile
- Setup a queue
- Create a requester favorites
- Disable users
- Transfer users

6.1 CREATE USER ACCOUNTS

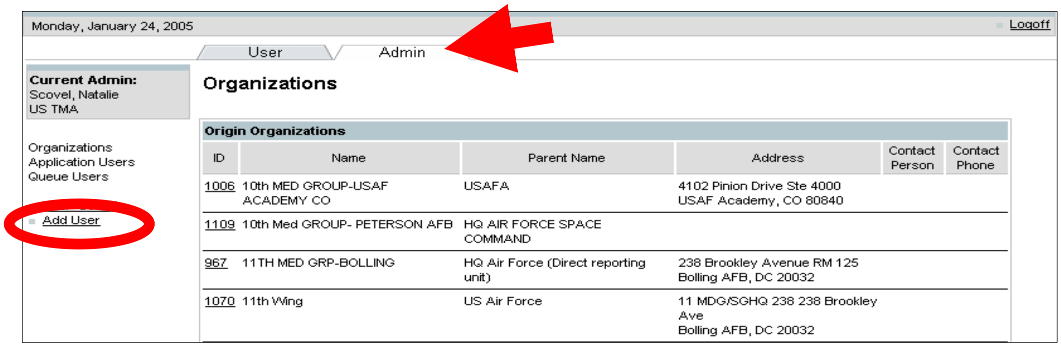
As a User Admin, you are responsible for adding users and assigning roles to users within your organization. Once the user has been added and assigned the appropriate organization and user role, provide the user with their login information. With this login, the new user will be able to access the application and perform appropriate functions.

To add users, you must log into PHIMT as a User Admin. Your User Admin account will have been established in advance by the Tool Admin. The Tool Admin only assigns a temporary password. Therefore, the first time you log in, you will be prompted to change your password. Once you have logged in, verify that the Current User shows your name and organization in the status box.

To add a user:

1. Select the Admin Tab on the PHIMT display screen.

2. Select the Add User hyperlink.



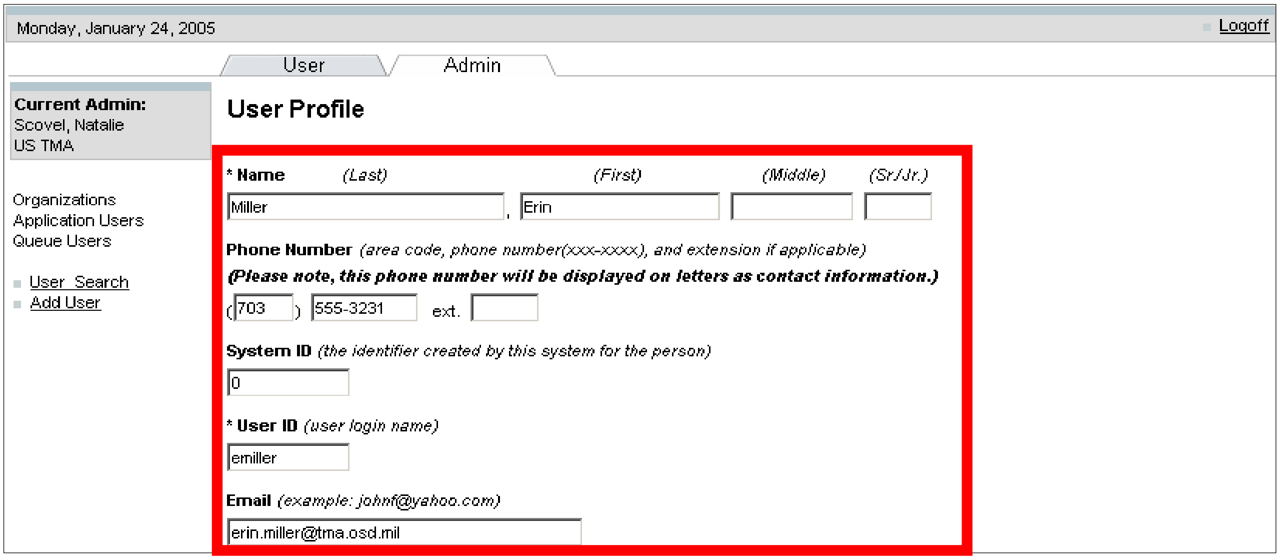
Organizations

Origin Organizations

ID	Name	Parent Name	Address	Contact Person	Contact Phone
1006	10th MED GROUP-USAF ACADEMY CO	USAFA	4102 Pinion Drive Ste 4000 USAF Academy, CO 80840		
1109	10th Med GROUP- PETERSON AFB	HQ AIR FORCE SPACE COMMAND			
967	11TH MED GRP-BOLLING	HQ Air Force (Direct reporting unit)	238 Brookley Avenue RM 125 Bolling AFB, DC 20032		
1070	11th Wing	US Air Force	11 MDG/SGHQ 238 238 Brookley Ave Bolling AFB, DC 20032		

3. Enter user information (name, phone number and email address).

4. Enter a unique User ID (No duplicate IDs are allowed across all Services).



Monday, January 24, 2005

Current Admin:
Scovel, Natalie
US TMA

User Profile

*** Name** *(Last)* *(First)* *(Middle)* *(Sr./Jr.)*
Miller, Erin

Phone Number *(area code, phone number(xxx-xxxx), and extension if applicable)*
(Please note, this phone number will be displayed on letters as contact information.)
(703) 555-3231 ext.

System ID *(the identifier created by this system for the person)*
0

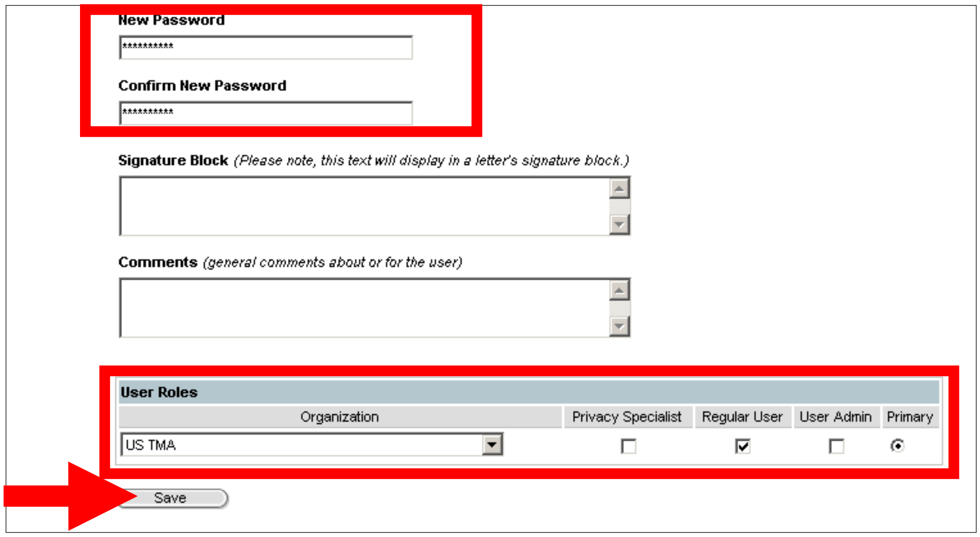
*** User ID** *(user login name)*
emiller

Email *(example: johnf@yahoo.com)*
erin.miller@tma.osd.mil

5. Enter a temporary new password and confirm new password.

6. Select organization from the drop-down box and select the appropriate user role.

7. Click on the Save button.



New Password
****

Confirm New Password
****

Signature Block *(Please note, this text will display in a letter's signature block.)*

Comments *(general comments about or for the user)*

User Roles

Organization	Privacy Specialist	Regular User	User Admin	Primary
US TMA	☐	☑	☐	●

6.2 ESTABLISH WORKFLOW

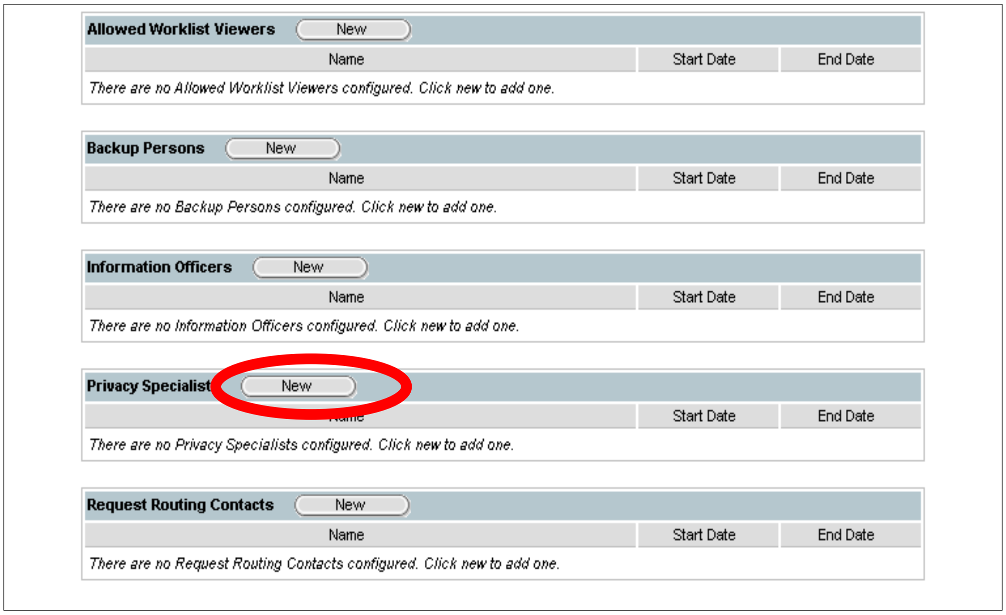
User-to-User relationships affect how requests are routed within PHIMT. These relationships need to be constructed in a manner that allows them the most use of all available Action Types shown on Request Action and Edit Activity screens. A typical request may be routed to a User Worklist, Privacy Specialist, or Other User. The User-to-User Relationships screen defines specific users who would be fulfilling these roles. This table shows the definitions of available user relationships.

User Relationship Definitions	
User Role	**Description**
Privacy Specialist	• Privacy Specialist is a user who is responsible for accepting and approving disclosure and disclosure accounting requests. • A Privacy Specialist for a regular user is usually someone from the same organization who is working in the Privacy Office. • A Privacy Specialist for a Privacy Specialist is a person at the high level who is working in the Central Privacy Office. *NOTE: The person selected as a Privacy Specialist should also have Privacy Specialist permission assigned to them by the User Admin.*
Backup Person	• Backup Person is a user who acts in your place whenever you are not able to attend to your requests due to being out of the office for business or pleasure, changing work priorities, or other reasons. • All outstanding requests assigned to you will be reassigned to your Backup Person at the time when the Backup Person relationship is assigned. • Any new requests will be routed to your Backup Person instead of you. You can assign a date when the Backup Person relationship should end or leave it open ended. *NOTE: End the Backup Person relationship as soon as you can resume working on your own requests.*

To set up a Workflow:

1. Scroll to the bottom of the User Profile screen (Regular User).

2. Click on the New button next to Privacy Specialists.



Allowed Worklist Viewers New

Name	Start Date	End Date

There are no Allowed Worklist Viewers configured. Click new to add one.

Backup Persons New

Name	Start Date	End Date

There are no Backup Persons configured. Click new to add one.

Information Officers New

Name	Start Date	End Date

There are no Information Officers configured. Click new to add one.

Privacy Specialist New

Name	Start Date	End Date

There are no Privacy Specialists configured. Click new to add one.

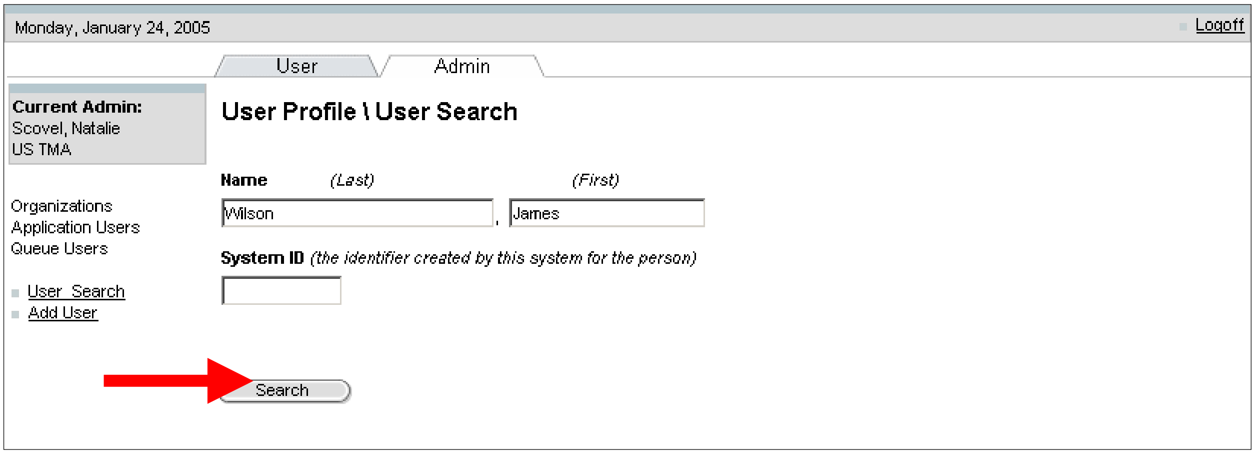
Request Routing Contacts New

Name	Start Date	End Date

There are no Request Routing Contacts configured. Click new to add one.

3. Enter Search Criteria.

4. Click on the Search button.



Current Admin:
Scovel, Natalie
US TMA

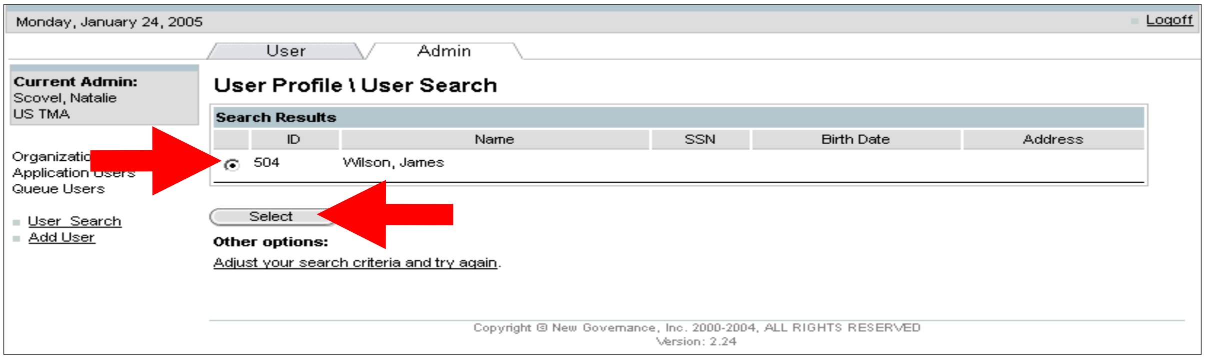
User Profile \ User Search

Name *(Last)* Wilson , *(First)* James

System ID *(the identifier created by this system for the person)*

*This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.*

7. Select the appropriate Privacy Specialist from the search results and click on the Select button.



Current Admin:
Scovel, Natalie
US TMA

Organizations
Application Users
Queue Users

- User Search
- Add User

User Profile \ User Search

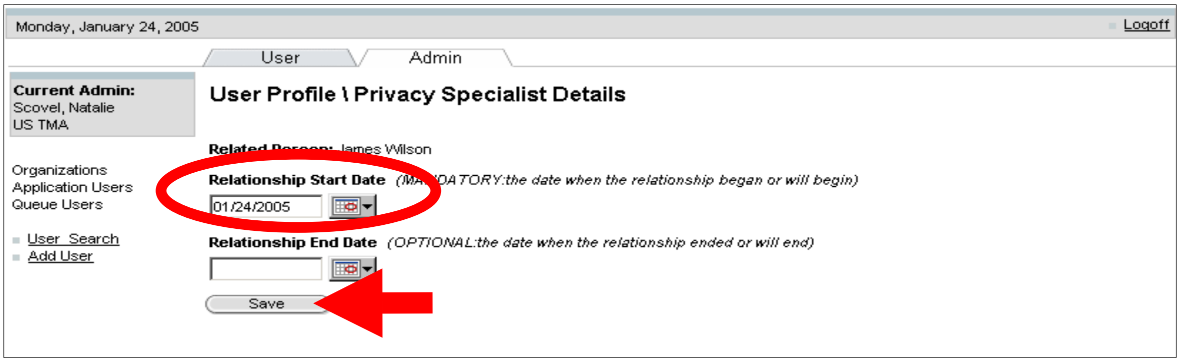
Search Results

	ID	Name	SSN	Birth Date	Address
●	504	Wilson, James			

Other options:
Adjust your search criteria and try again.

6. Set the Relationship Start Date/End Date. (The end date is optional).\

7. Click on the Save button.



Current Admin:
Scovel, Natalie
US TMA

Organizations
Application Users
Queue Users

- User Search
- Add User

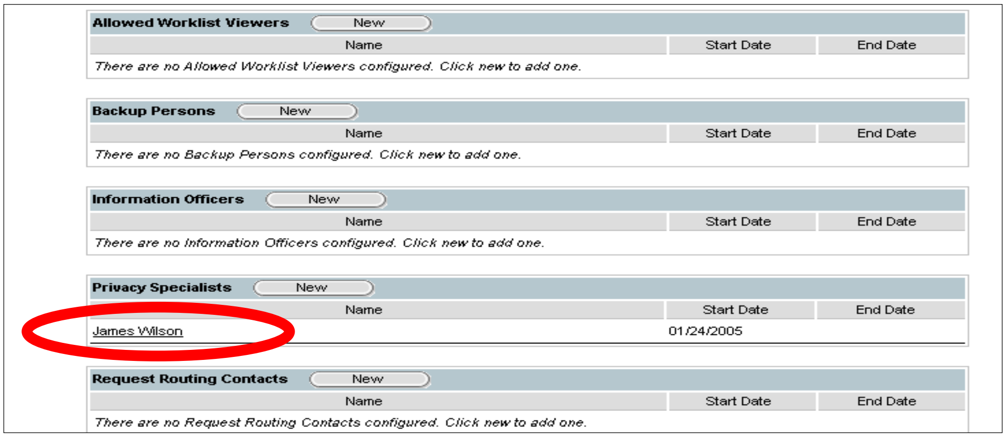
User Profile \ Privacy Specialist Details

Related Person: James Wilson

Relationship Start Date *(MANDATORY:the date when the relationship began or will begin)*
01/24/2005

Relationship End Date *(OPTIONAL:the date when the relationship ended or will end)*

The Privacy Specialist is added to the User Profile screen.



Allowed Worklist Viewers New

Name	Start Date	End Date
There are no Allowed Worklist Viewers configured. Click new to add one.		

Backup Persons New

Name	Start Date	End Date
There are no Backup Persons configured. Click new to add one.		

Information Officers New

Name	Start Date	End Date
There are no Information Officers configured. Click new to add one.		

Privacy Specialists New

Name	Start Date	End Date
James Wilson	01/24/2005	

Request Routing Contacts New

Name	Start Date	End Date
There are no Request Routing Contacts configured. Click new to add one.		

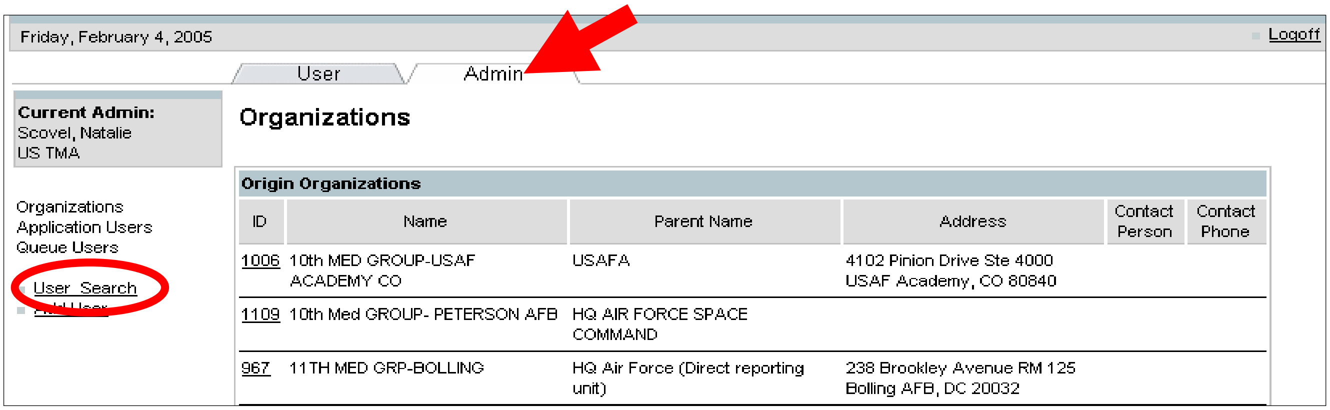
6.3 Edit User Profile

The User Admin has the ability to edit user profiles for individuals within their organization. Changes can be made to any of the fields in the User Profile screen with the exception of the System ID. The System ID is a computer-generated number, which cannot be changed.

To edit a user's profile:

1. Select the Admin Tab.

2. Click on the User Search hyperlink.



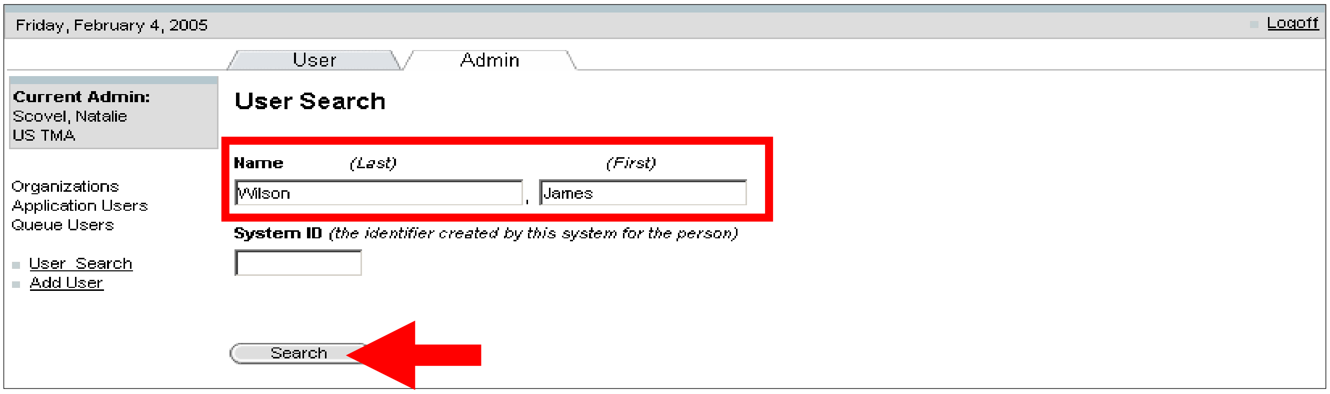
Organizations

Origin Organizations

ID	Name	Parent Name	Address	Contact Person	Contact Phone
1006	10th MED GROUP-USAF ACADEMY CO	USAFA	4102 Pinion Drive Ste 4000 USAF Academy, CO 80840		
1109	10th Med GROUP- PETERSON AFB	HQ AIR FORCE SPACE COMMAND			
967	11TH MED GRP-BOLLING	HQ Air Force (Direct reporting unit)	238 Brookley Avenue RM 125 Bolling AFB, DC 20032		

3. Type in the Search Criteria.

4. Click on the Search button.



User Search

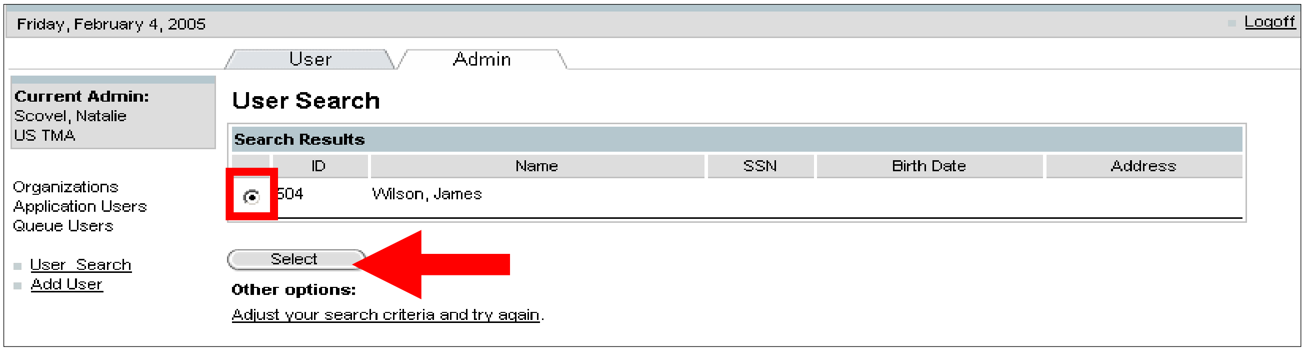
Name (Last) (First)

Wilson , James

System ID (the identifier created by this system for the person)

This document contains proprietary information and will be handled within Government regulations. It is intended solely for the use and information of the Military Health System.

5. Select the appropriate user from the search results screen.



Current Admin:
Scovel, Natalie
US TMA

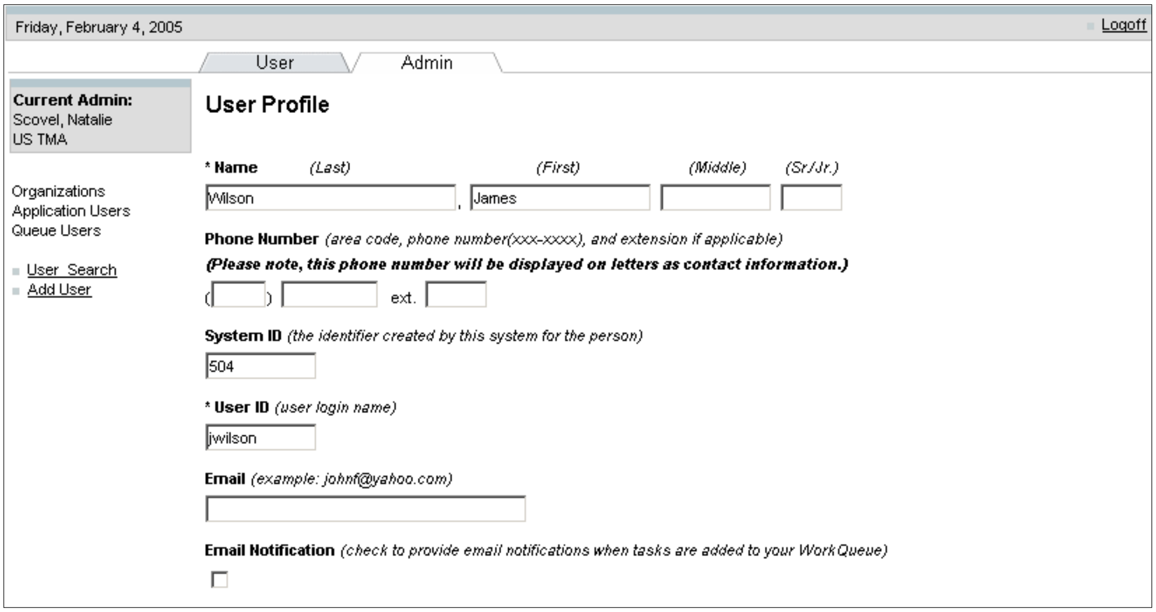
User Search

Search Results

	ID	Name	SSN	Birth Date	Address
●	504	Wilson, James			

Other options:

6. Update the User Profile Screen. (Changes can be made to any of the fields in the User Profile screen, except the System ID).



Current Admin:
Scovel, Natalie
US TMA

User Profile

* **Name** *(Last)* *(First)* *(Middle)* *(Sr/Jr.)*
Wilson , James

Phone Number *(area code, phone number(xxx-xxxx), and extension if applicable)*
(Please note, this phone number will be displayed on letters as contact information.)
( ) ext.

System ID *(the identifier created by this system for the person)*
504

* **User ID** *(user login name)*
jwilson

Email *(example: johnf@yahoo.com)*

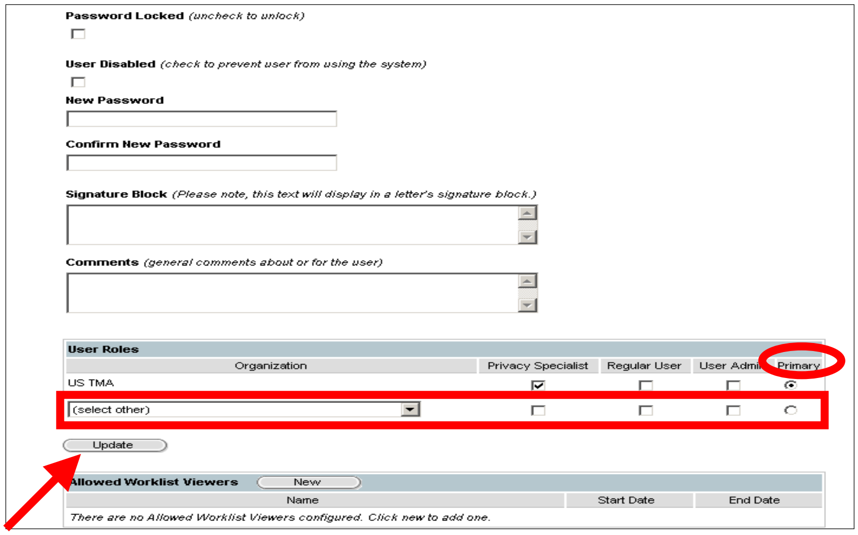
Email Notification *(check to provide email notifications when tasks are added to your WorkQueue)*
□

You can change or create a new Organization and User Role by selecting an organization from the drop-down menu in the User Roles section. (A user can have multiple roles in multiple organizations).

7. Scroll down to the bottom of the screen.

8. Select the organization and the appropriate User Role checkbox. If the new Role and Organization should be the primary then choose the small circle radio button.

9. Click on the Update button.



Password Locked *(uncheck to unlock)*

□

User Disabled *(check to prevent user from using the system)*

□

New Password

Confirm New Password

Signature Block *(Please note, this text will display in a letter's signature block.)*

Comments *(general comments about or for the user)*

User Roles

Organization	Privacy Specialist	Regular User	User Admi	Primary
US TMA	☑	□	□	●
(select other)	□	□	□	○

Allowed Worklist Viewers

Name	Start Date	End Date

There are no Allowed Worklist Viewers configured. Click new to add one.

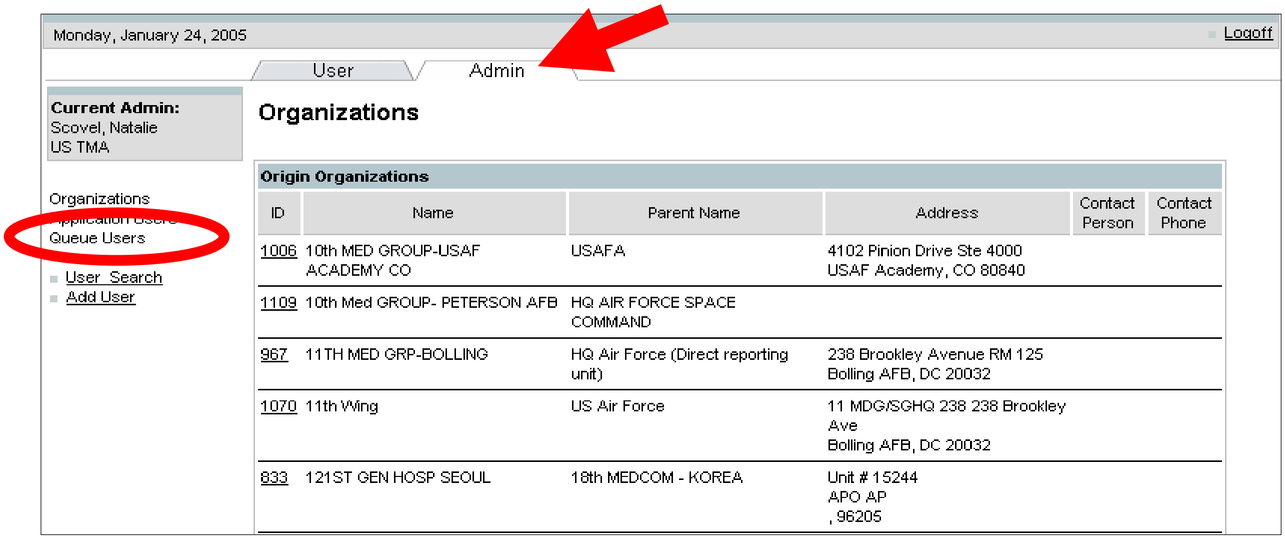
6.4 Queue Setup

A queue is a distribution list for a specific organization that is comprised of two or more Privacy Specialists. The User Admin at the local command is responsible for setting up a queue. Queues are created to expedite the process of approving/denying a disclosure. Only users affiliated with a given organization will see that organization's routing options.

To setup a queue:

1. Select the Admin Tab.

2. Select the Queue Users hyperlink.



Monday, January 24, 2005

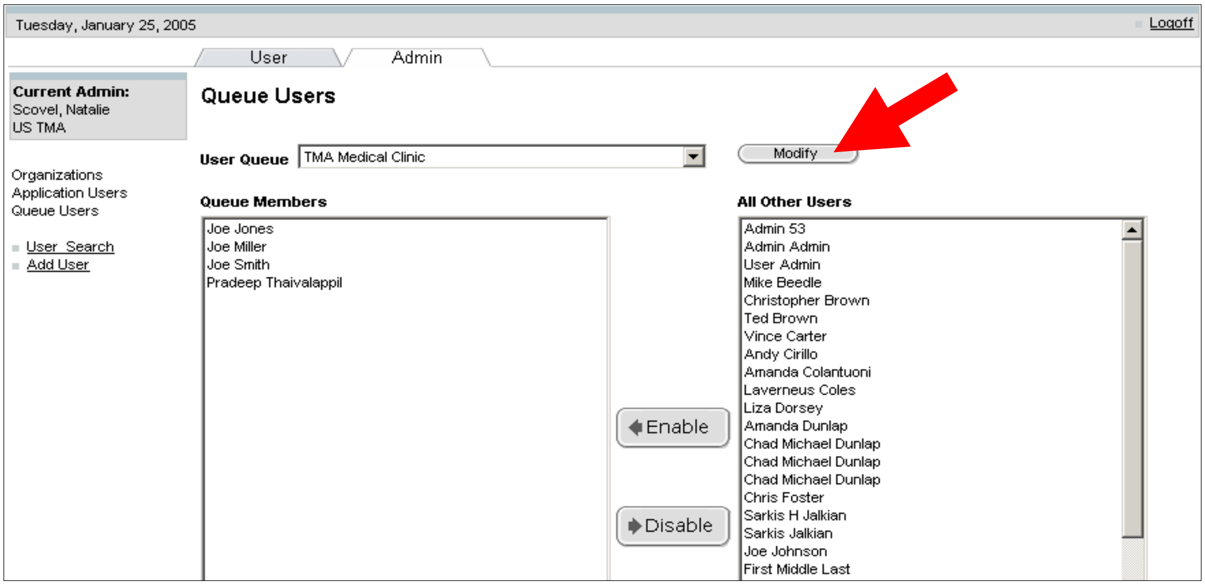
Current Admin:
Scovel, Natalie
US TMA

Organizations

Origin Organizations

ID	Name	Parent Name	Address	Contact Person	Contact Phone
1006	10th MED GROUP-USAF ACADEMY CO	USAFA	4102 Pinion Drive Ste 4000 USAF Academy, CO 80840		
1109	10th Med GROUP- PETERSON AFB	HQ AIR FORCE SPACE COMMAND			
967	11TH MED GRP-BOLLING	HQ Air Force (Direct reporting unit)	238 Brookley Avenue RM 125 Bolling AFB, DC 20032		
1070	11th Wing	US Air Force	11 MDG/SGHQ 238 238 Brookley Ave Bolling AFB, DC 20032		
833	121ST GEN HOSP SEOUL	18th MEDCOM - KOREA	Unit # 15244 APO AP , 96205		

3. Click on the Modify button to add a new queue.



Current Admin:
Scovel, Natalie
US TMA

Queue Users

User Queue TMA Medical Clinic

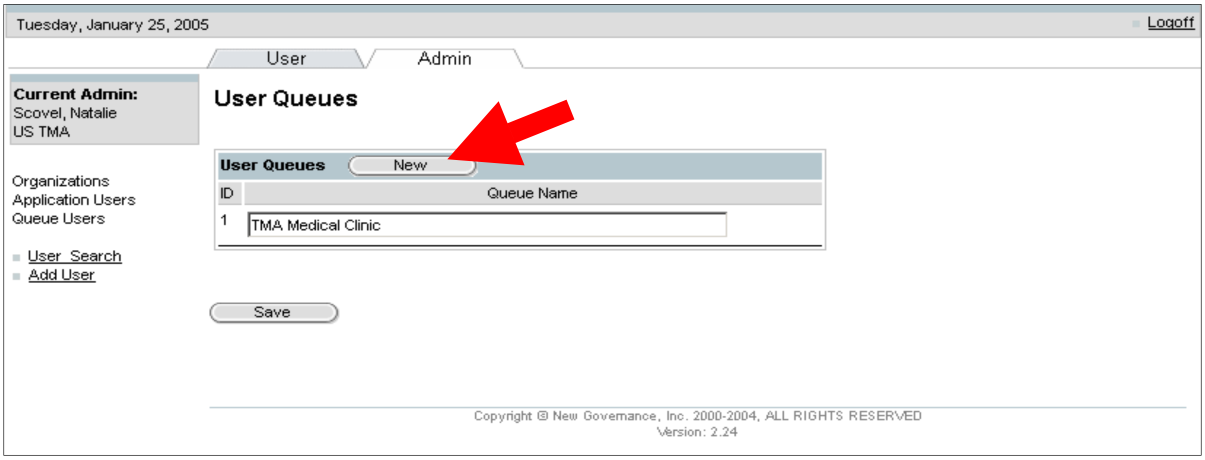
Queue Members

Joe Jones
Joe Miller
Joe Smith
Pradeep Thaivalappil

All Other Users

Admin 53
Admin Admin
User Admin
Mike Beedle
Christopher Brown
Ted Brown
Vince Carter
Andy Cirillo
Amanda Colantuoni
Laverneus Coles
Liza Dorsey
Amanda Dunlap
Chad Michael Dunlap
Chad Michael Dunlap
Chad Michael Dunlap
Chris Foster
Sarkis H Jalkian
Sarkis Jalkian
Joe Johnson
First Middle Last

4. Click on the New button.



Current Admin:
Scovel, Natalie
US TMA

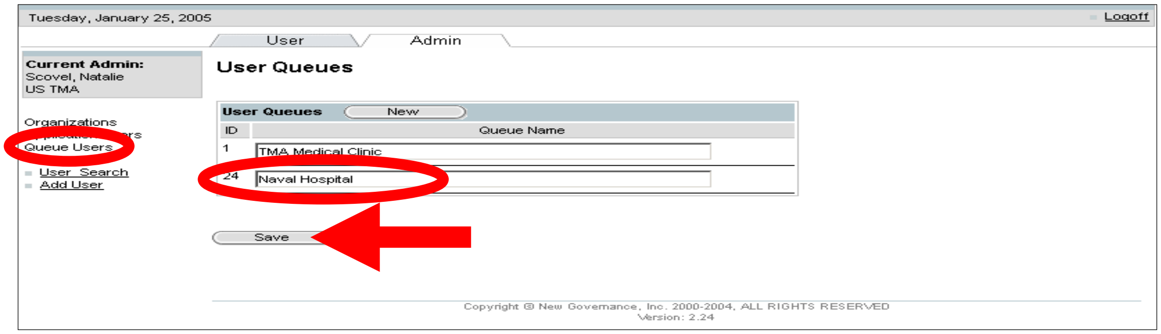
User Queues

User Queues	
ID	Queue Name
1	TMA Medical Clinic

5. Enter the description of the Queue in the text box.

6. Click on the Save button

7. Once saved, select the Queue Users hyperlink.

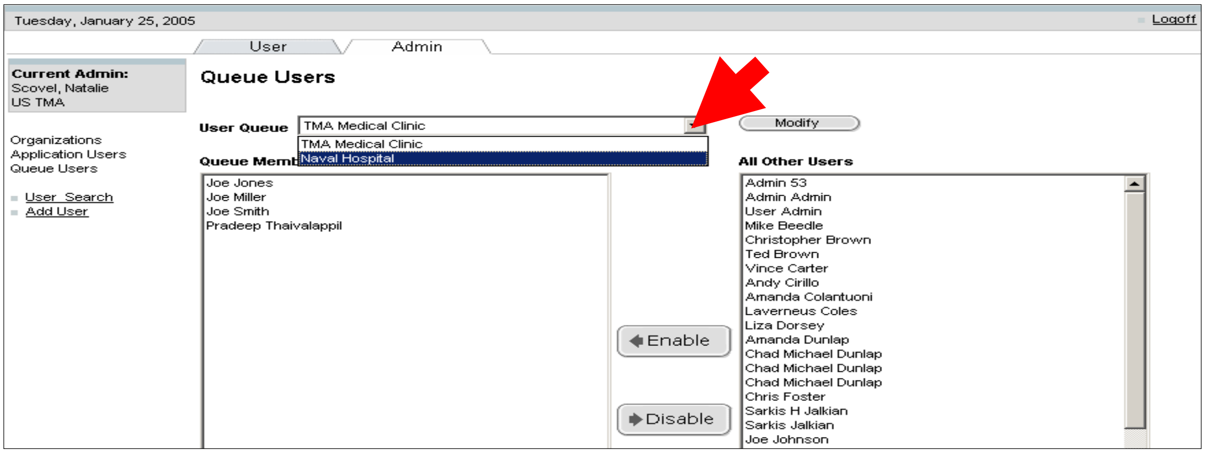


User Queues

ID	Queue Name
1	TMA Medical Clinic
24	Naval Hospital

Copyright © New Governance, Inc. 2000-2004, ALL RIGHTS RESERVED
Version: 2.24

8. Select the Queue you created from the drop-down box.



Queue Users

User Queue: TMA Medical Clinic

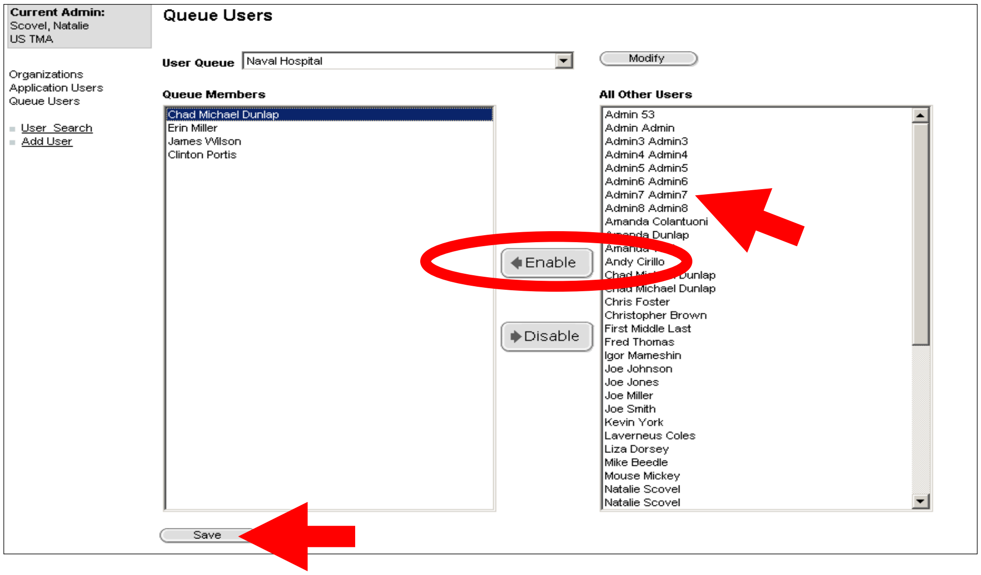
TMA Medical Clinic
Naval Hospital

Queue Members:
Joe Jones
Joe Miller
Joe Smith
Pradeep Thaivalappil

All Other Users:
Admin 53
Admin Admin
User Admin
Mike Beedle
Christopher Brown
Ted Brown
Vince Carter
Andy Cirillo
Amanda Colantuoni
Laverneus Coles
Liza Dorsey
Amanda Dunlap
Chad Michael Dunlap
Chad Michael Dunlap
Chad Michael Dunlap
Chris Foster
Sarkis H Jalkian
Sarkis Jalkian
Joe Johnson

9. Select the users that you want to add to the queue and click on Enable.

10. Click on the Save button.



Queue Users

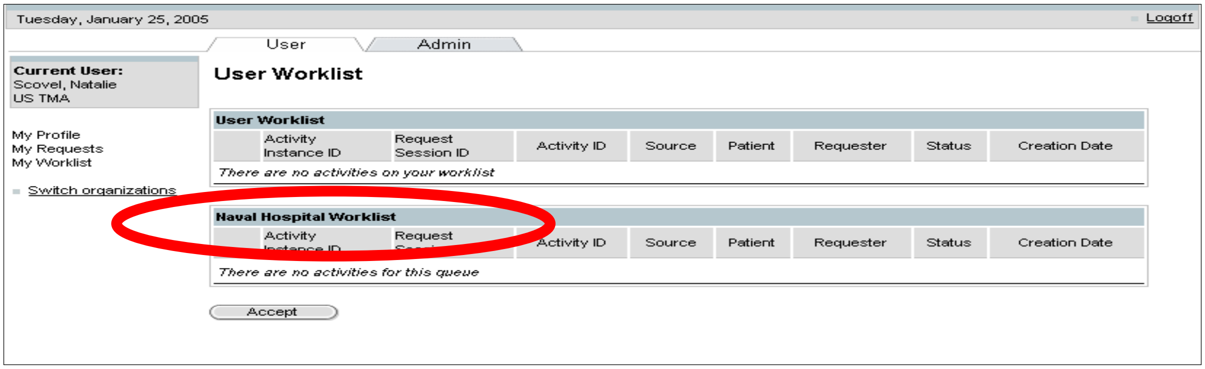
User Queue: Naval Hospital

Queue Members:
Chad Michael Dunlap
Erin Miller
James Wilson
Clinton Portis

All Other Users:
Admin 53
Admin Admin
Admin3 Admin3
Admin4 Admin4
Admin5 Admin5
Admin6 Admin6
Admin7 Admin7
Admin8 Admin8
Amanda Colantuoni
Amanda Dunlap
Amanda
Andy Cirillo
Chad Michael Dunlap
Chad Michael Dunlap
Chris Foster
Christopher Brown
First Middle Last
Fred Thomas
Igor Mameshin
Joe Johnson
Joe Jones
Joe Miller
Joe Smith
Kevin York
Laverneus Coles
Liza Dorsey
Mike Beedle
Mouse Mickey
Natalie Scovel
Natalie Scovel

This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.

- The queue that you added will show up in the user's worklist.



Current User:
Scovel, Natalie
US TMA

My Profile
My Requests
My Worklist

Switch organizations

User Worklist

User Worklist

	Activity Instance ID	Request Session ID	Activity ID	Source	Patient	Requester	Status	Creation Date
There are no activities on your worklist								

Naval Hospital Worklist

	Activity Instance ID	Request Session ID	Activity ID	Source	Patient	Requester	Status	Creation Date
There are no activities for this queue								

6.5 REQUESTER FAVORITES

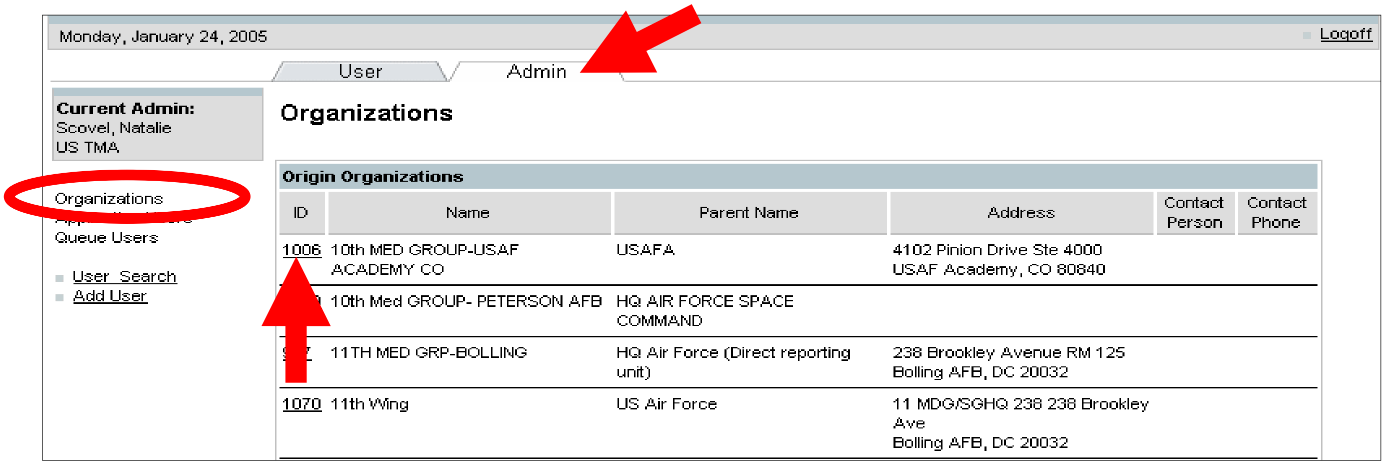
An organization can create a list of requester "favorites" that show up in the requester drop-down list. User Admins can set up the list of favorites per organization. If an organization name is not in the favorites list, the user will be allowed to search for it manually. A given "requester" can appear in multiple "favorites" lists.

To set up an organization's requester favorites:

1. Select the Admin Tab.

2. Select the Organization's hyperlink.

3. Select the ID hyperlink for your Origin Organization.



Current Admin:
Scovel, Natalie
US TMA

Organizations
Application Users
Queue Users

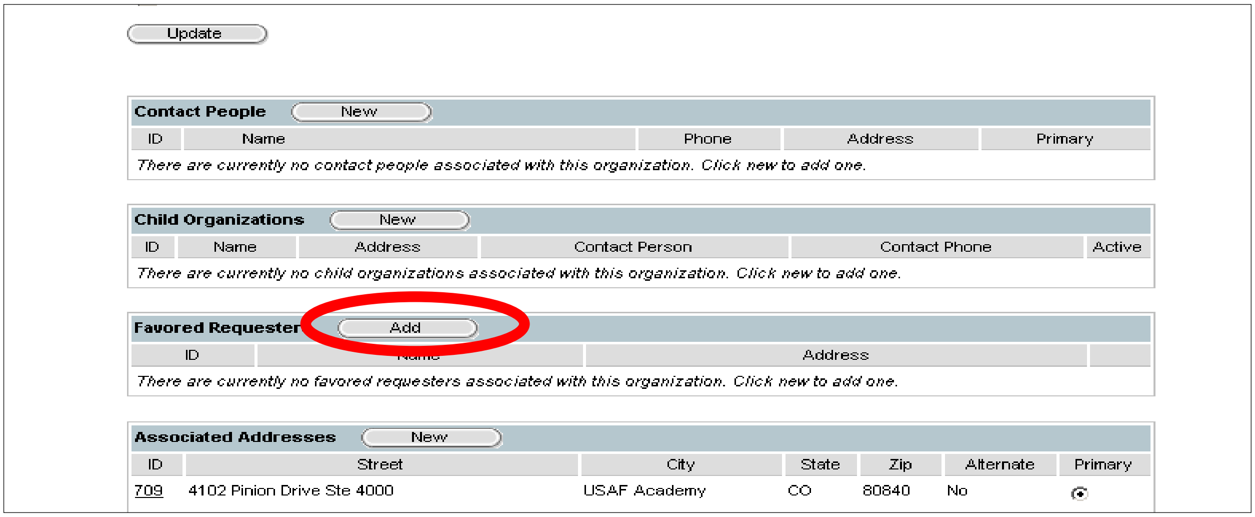
User Search
Add User

Organizations

Origin Organizations

ID	Name	Parent Name	Address	Contact Person	Contact Phone
1006	10th MED GROUP-USAF ACADEMY CO	USAFA	4102 Pinion Drive Ste 4000 USAF Academy, CO 80840		
[illegible]	10th Med GROUP- PETERSON AFB	HQ AIR FORCE SPACE COMMAND			
[illegible]	11TH MED GRP-BOLLING	HQ Air Force (Direct reporting unit)	238 Brookley Avenue RM 125 Bolling AFB, DC 20032		
1070	11th Wing	US Air Force	11 MDG/SGHQ 238 238 Brookley Ave Bolling AFB, DC 20032		

4. Scroll down to Favored Requesters and click on the Add button.



Update

Contact People New

ID	Name	Phone	Address	Primary
There are currently no contact people associated with this organization. Click new to add one.				

Child Organizations New

ID	Name	Address	Contact Person	Contact Phone	Active
There are currently no child organizations associated with this organization. Click new to add one.					

Favored Requester Add

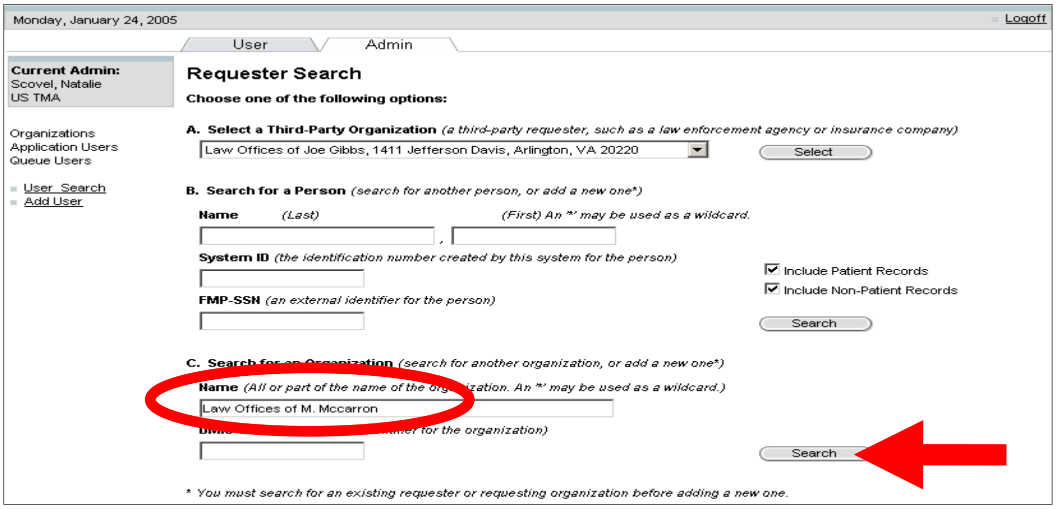
ID	Name	Address	
There are currently no favored requesters associated with this organization. Click new to add one.			

Associated Addresses New

ID	Street	City	State	Zip	Alternate	Primary
709	4102 Pinion Drive Ste 4000	USAF Academy	CO	80840	No	●

5. Enter organization search criteria.

6. Click on the Search button.



Monday, January 24, 2005 Logoff

User Admin

Current Admin:
Scovel, Natalie
US TMA

Organizations
Application Users
Queue Users

- User Search
- Add User

Requester Search

Choose one of the following options:

A. Select a Third-Party Organization *(a third-party requester, such as a law enforcement agency or insurance company)*

Law Offices of Joe Gibbs, 1411 Jefferson Davis, Arlington, VA 20220 ▼ Select

B. Search for a Person *(search for another person, or add a new one*)*

Name *(Last)* *(First) An '*' may be used as a wildcard.*

System ID *(the identification number created by this system for the person)*

☑ Include Patient Records
☑ Include Non-Patient Records

FMP-SSN *(an external identifier for the person)*

Search

C. Search for an Organization *(search for another organization, or add a new one*)*

Name *(All or part of the name of the organization. An '*' may be used as a wildcard.)*

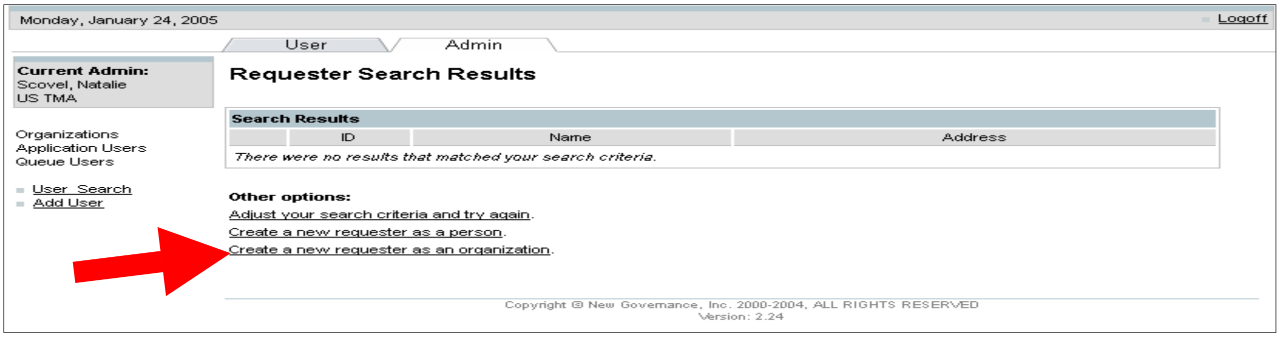
Law Offices of M. Mccarron

DMIS *(an external identifier for the organization)*

Search

** You must search for an existing requester or requesting organization before adding a new one.*

7. If the requester is not found, click on the “Create a new requester as an Organization”.



Monday, January 24, 2005 Logoff

User Admin

Current Admin:
Scovel, Natalie
US TMA

Organizations
Application Users
Queue Users

- User Search
- Add User

Requester Search Results

Search Results

	ID	Name	Address
There were no results that matched your search criteria.			

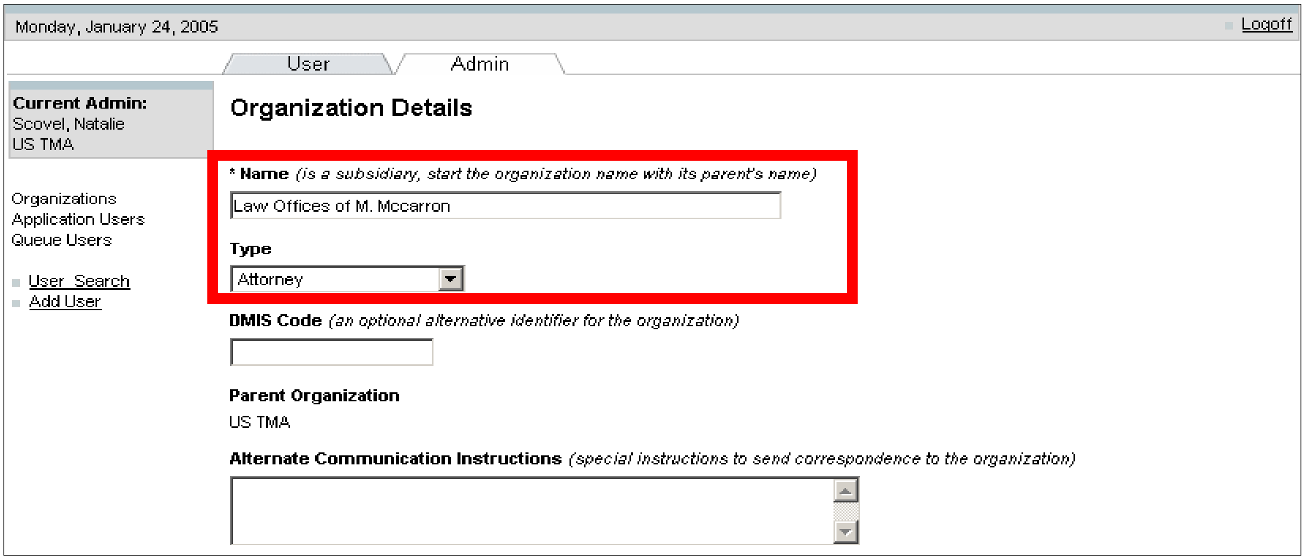
Other options:

Adjust your search criteria and try again.
Create a new requester as a person.
Create a new requester as an organization.

Copyright © New Governance, Inc. 2000-2004, ALL RIGHTS RESERVED
Version: 2.24

8. Enter the name of the Organization.

9. Select the organization type from the drop-down box.



Monday, January 24, 2005

Current Admin:
Scovel, Natalie
US TMA

Organization Details

* **Name** *(is a subsidiary, start the organization name with its parent's name)*

Law Offices of M. Mccarron

Type

Attorney

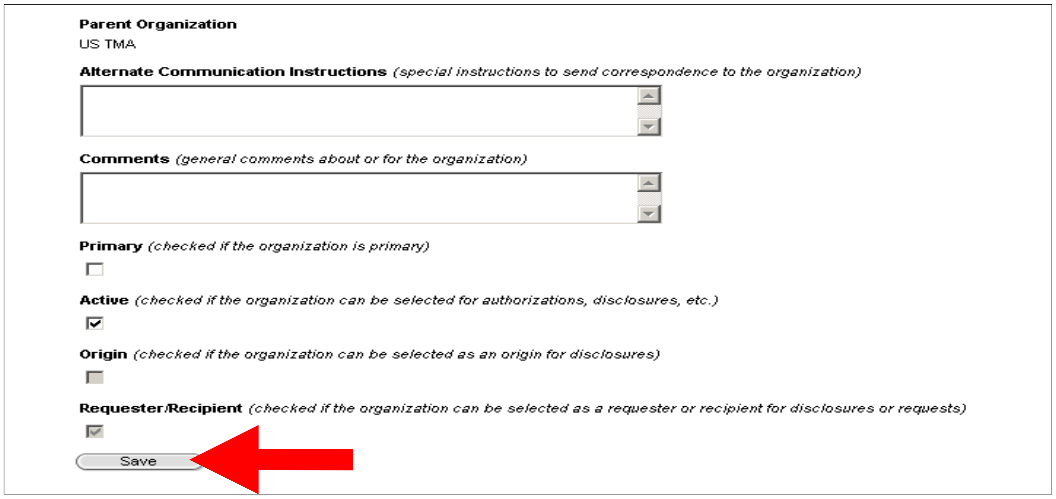
DMIS Code *(an optional alternative identifier for the organization)*

Parent Organization

US TMA

Alternate Communication Instructions *(special instructions to send correspondence to the organization)*

10. Scroll down to the bottom of the screen and click on the Save button.



Parent Organization

US TMA

Alternate Communication Instructions *(special instructions to send correspondence to the organization)*

Comments *(general comments about or for the organization)*

Primary *(checked if the organization is primary)*

□

Active *(checked if the organization can be selected for authorizations, disclosures, etc.)*

☑

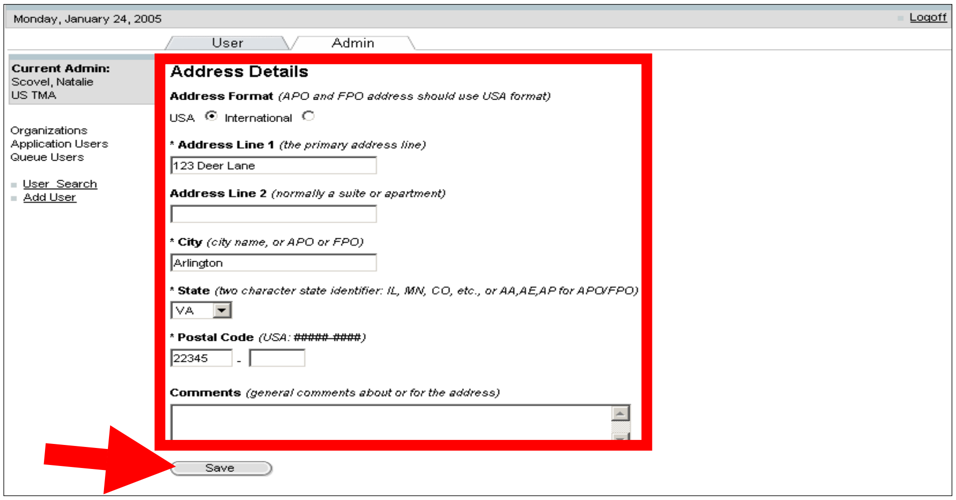
Origin *(checked if the organization can be selected as an origin for disclosures)*

□

Requester/Recipient *(checked if the organization can be selected as a requester or recipient for disclosures or requests)*

☑

11. Enter the Organization Address Details and click on the Save button.



Address Details

Address Format *(APO and FPO address should use USA format)*

USA ● International ○

* **Address Line 1** *(the primary address line)*

123 Deer Lane

Address Line 2 *(normally a suite or apartment)*

* **City** *(city name, or APO or FPO)*

Arlington

* **State** *(two character state identifier: IL, MN, CO, etc., or AA,AE,AP for APO/FPO)*

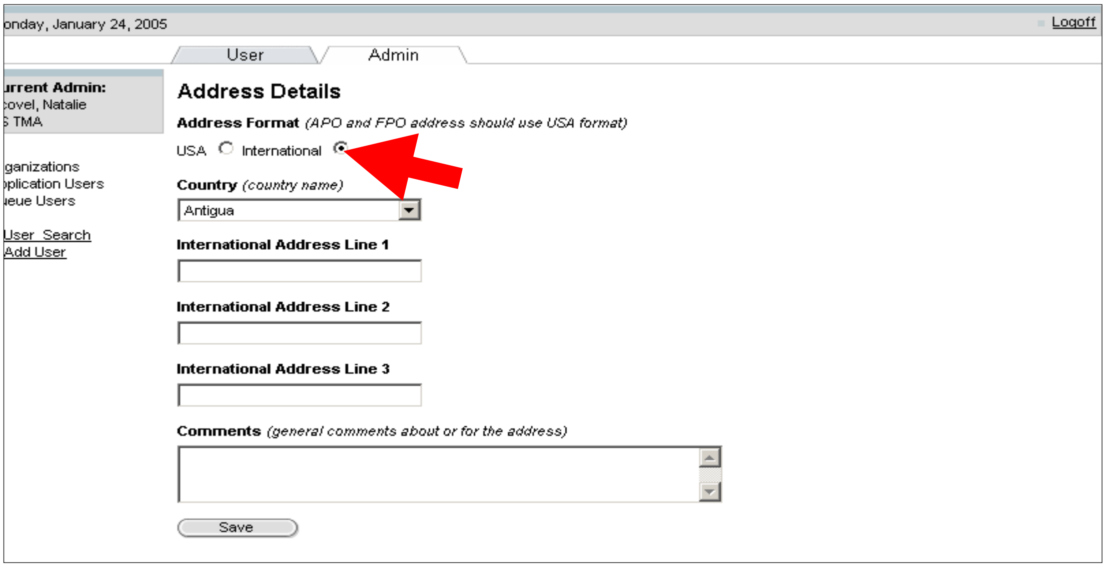
VA

* **Postal Code** *(USA: #####-####)*

22345 -

Comments *(general comments about or for the address)*

- If you are entering an International Address, select the International radio button.



Address Details

Address Format *(APO and FPO address should use USA format)*

USA ○ International ●

Country *(country name)*

Antigua

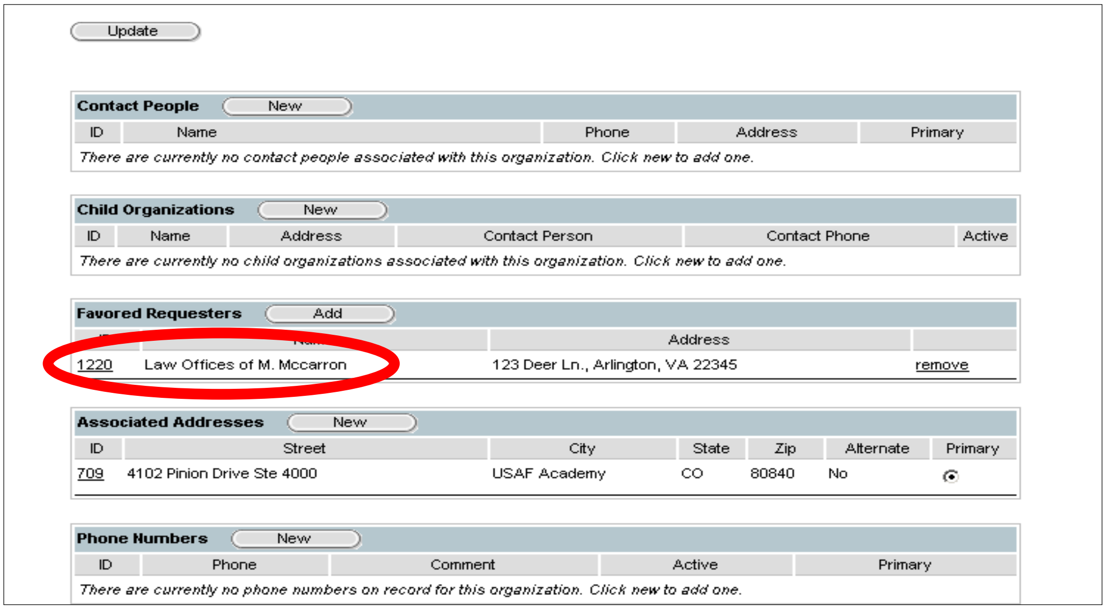
International Address Line 1

International Address Line 2

International Address Line 3

Comments *(general comments about or for the address)*

- The organization that you added now appears in your requester favorites.



Contact People

ID	Name	Phone	Address	Primary

There are currently no contact people associated with this organization. Click new to add one.

Child Organizations

ID	Name	Address	Contact Person	Contact Phone	Active

There are currently no child organizations associated with this organization. Click new to add one.

Favored Requesters

ID	Name	Address	
1220	Law Offices of M. Mccarron	123 Deer Ln., Arlington, VA 22345	remove

Associated Addresses

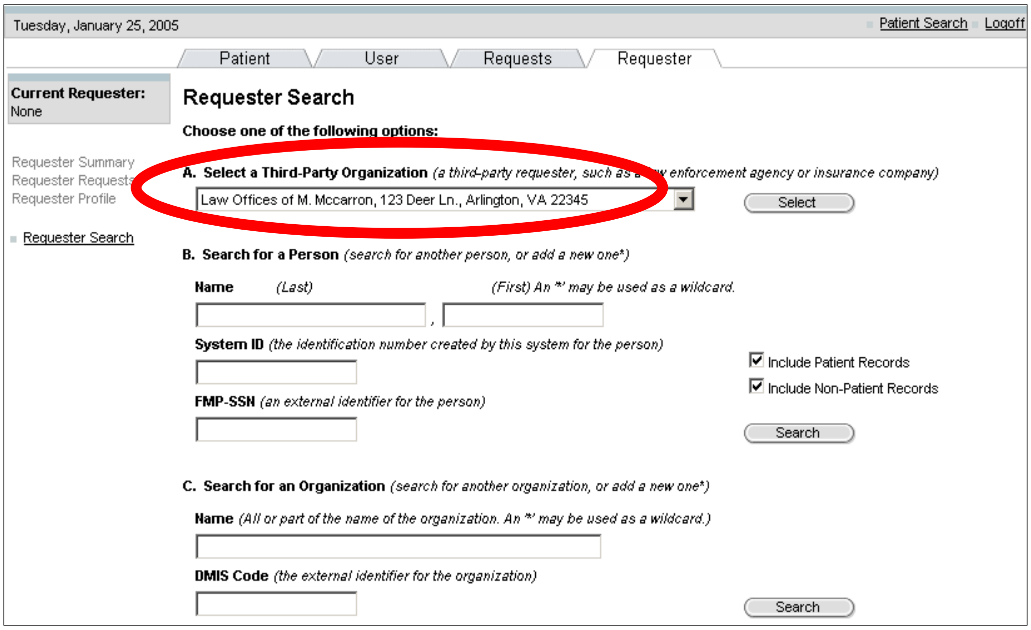
ID	Street	City	State	Zip	Alternate	Primary
709	4102 Pinion Drive Ste 4000	USAF Academy	CO	80840	No	●

Phone Numbers

ID	Phone	Comment	Active	Primary

There are currently no phone numbers on record for this organization. Click new to add one.

- When logging in as a Regular User, the organization that you added will appear in the requester favorites drop-down box for your organization.



Tuesday, January 25, 2005

Current Requester: None

Requester Search

Choose one of the following options:

A. Select a Third-Party Organization *(a third-party requester, such as a law enforcement agency or insurance company)*

Law Offices of M. Mccarron, 123 Deer Ln., Arlington, VA 22345

B. Search for a Person *(search for another person, or add a new one*)*

Name *(Last)* *(First) An '*' may be used as a wildcard.*

System ID *(the identification number created by this system for the person)*

FMP-SSN *(an external identifier for the person)*

☑ Include Patient Records

☑ Include Non-Patient Records

C. Search for an Organization *(search for another organization, or add a new one*)*

Name *(All or part of the name of the organization. An '*' may be used as a wildcard.)*

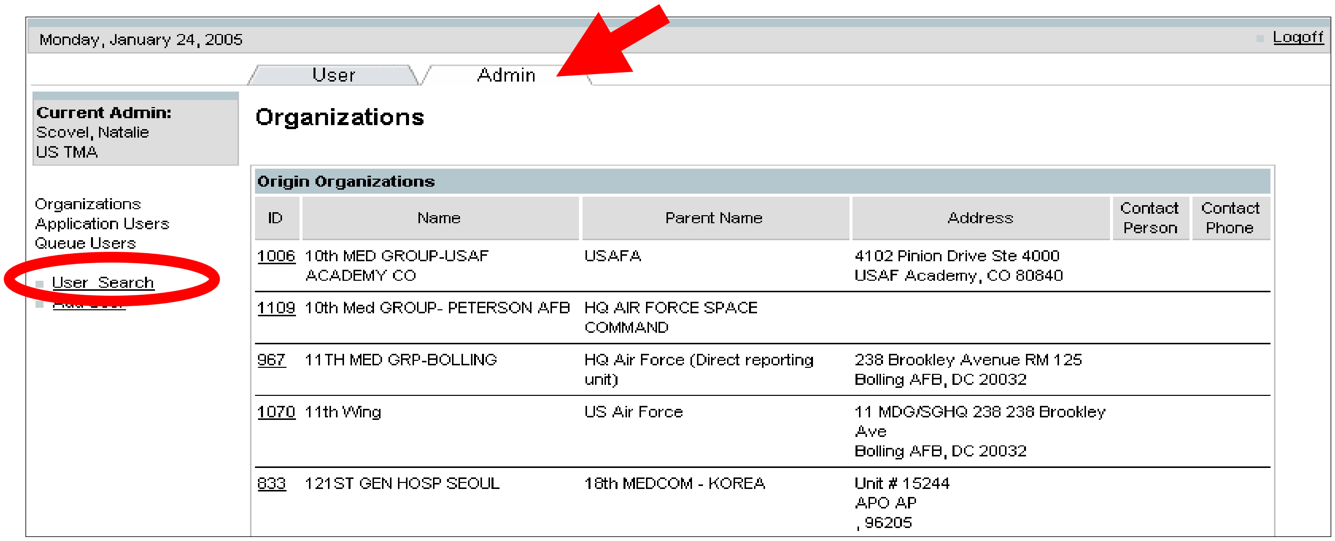
DMIS Code *(the external identifier for the organization)*

6.6 DISABLING USERS

If a user transfers to another facility or separates from the Service, the User Admin needs to disable that individual's ability to access the tool. You cannot delete users from the system due to future auditing, disclosure tracking, and users are attached to the records they created.

To disable a user:

1. Select the Admin Tab
2. Select the User Search hyperlink.



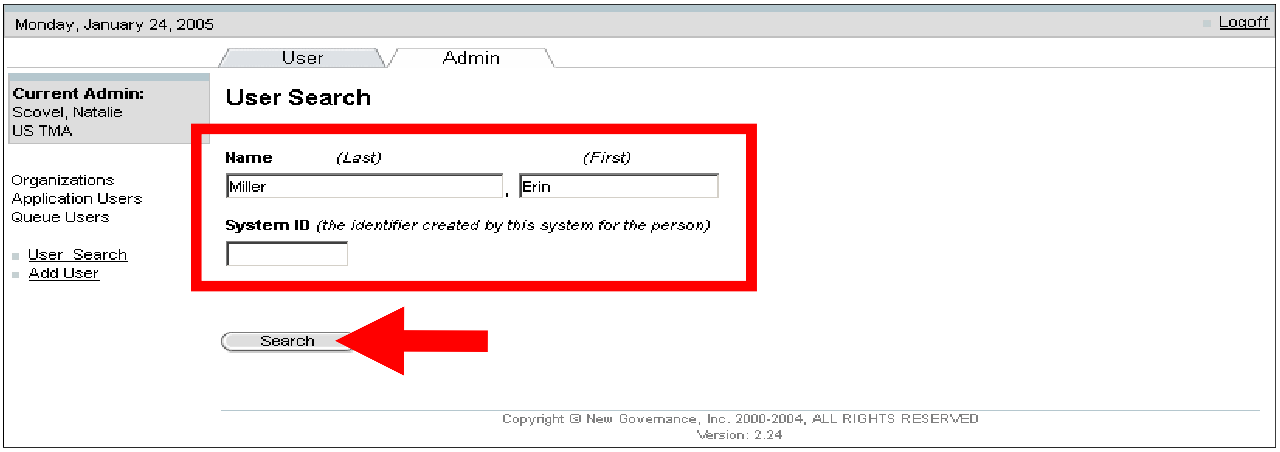
Current Admin:
Scovel, Natalie
US TMA

Organizations

Origin Organizations

ID	Name	Parent Name	Address	Contact Person	Contact Phone
1006	10th MED GROUP-USAF ACADEMY CO	USAFA	4102 Pinion Drive Ste 4000 USAF Academy, CO 80840		
1109	10th Med GROUP- PETERSON AFB	HQ AIR FORCE SPACE COMMAND			
967	11TH MED GRP-BOLLING	HQ Air Force (Direct reporting unit)	238 Brookley Avenue RM 125 Bolling AFB, DC 20032		
1070	11th Wing	US Air Force	11 MDG/SGHQ 238 238 Brookley Ave Bolling AFB, DC 20032		
833	121ST GEN HOSP SEOUL	18th MEDCOM - KOREA	Unit # 15244 APO AP , 96205		

3. Enter the Search Criteria.
4. Click on the Search button.



Current Admin:
Scovel, Natalie
US TMA

User Search

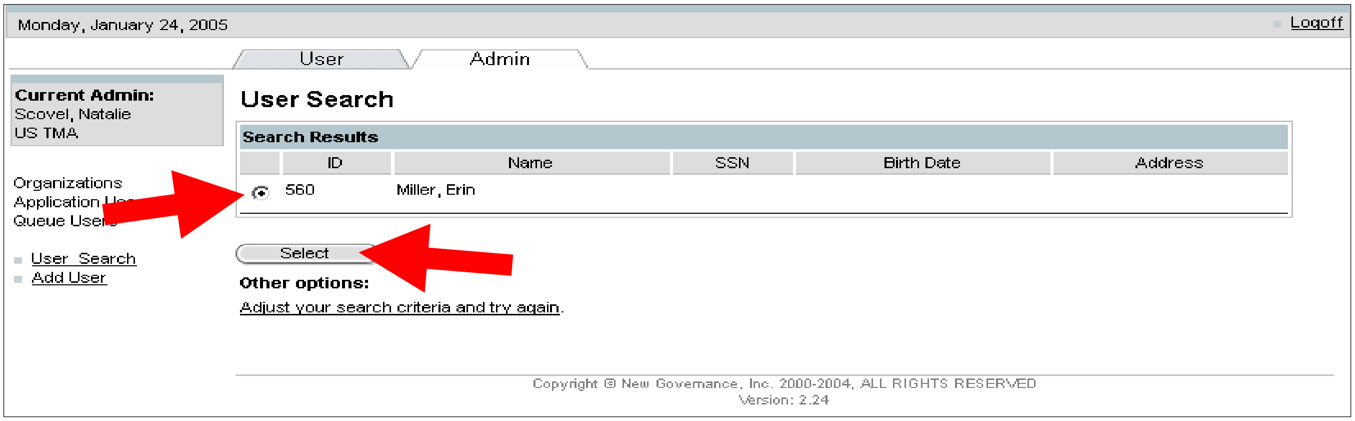
Name *(Last)* Miller, *(First)* Erin

System ID *(the identifier created by this system for the person)*

Copyright © New Governance, Inc. 2000-2004, ALL RIGHTS RESERVED
Version: 2.24

5. Click on the radio button next to the user to be disabled.

6. Click on the Select button.



Monday, January 24, 2005

Current Admin:
Scovel, Natalie
US TMA

User Search

Search Results

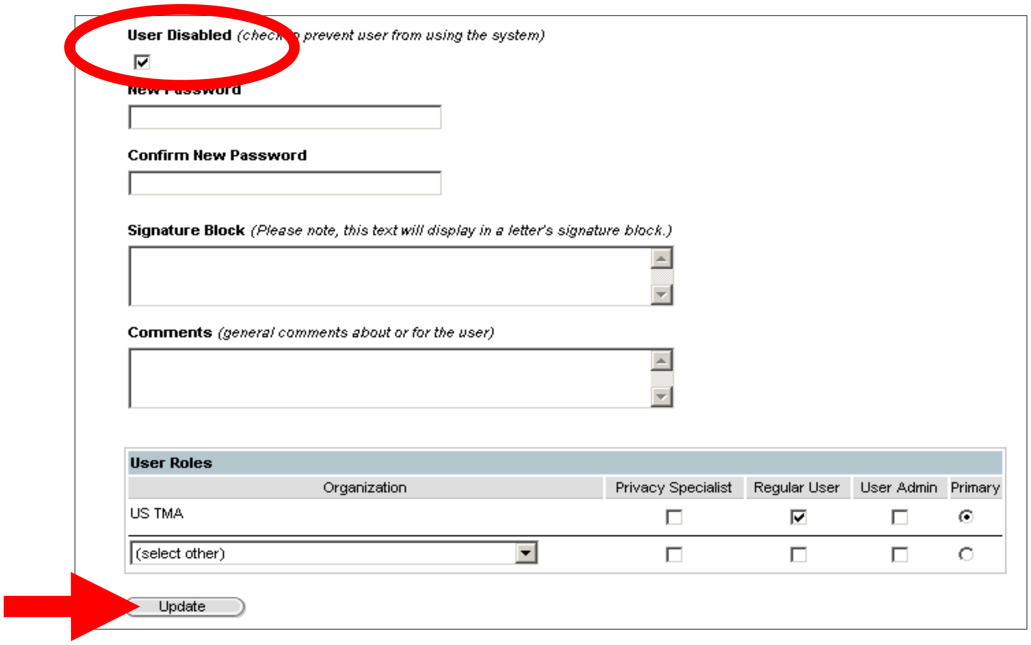
	ID	Name	SSN	Birth Date	Address
●	560	Miller, Erin			

Other options:
Adjust your search criteria and try again.

Copyright © New Governance, Inc. 2000-2004, ALL RIGHTS RESERVED
Version: 2.24

7. Scroll down and place a check in the “User Disabled” box.

8. Click on the Update button.



User Disabled *(check to prevent user from using the system)*
☑

New Password

Confirm New Password

Signature Block *(Please note, this text will display in a letter's signature block.)*

Comments *(general comments about or for the user)*

User Roles

Organization	Privacy Specialist	Regular User	User Admin	Primary
US TMA	□	☑	□	●
(select other)	□	□	□	○

6.7 TRANSFERRING USERS

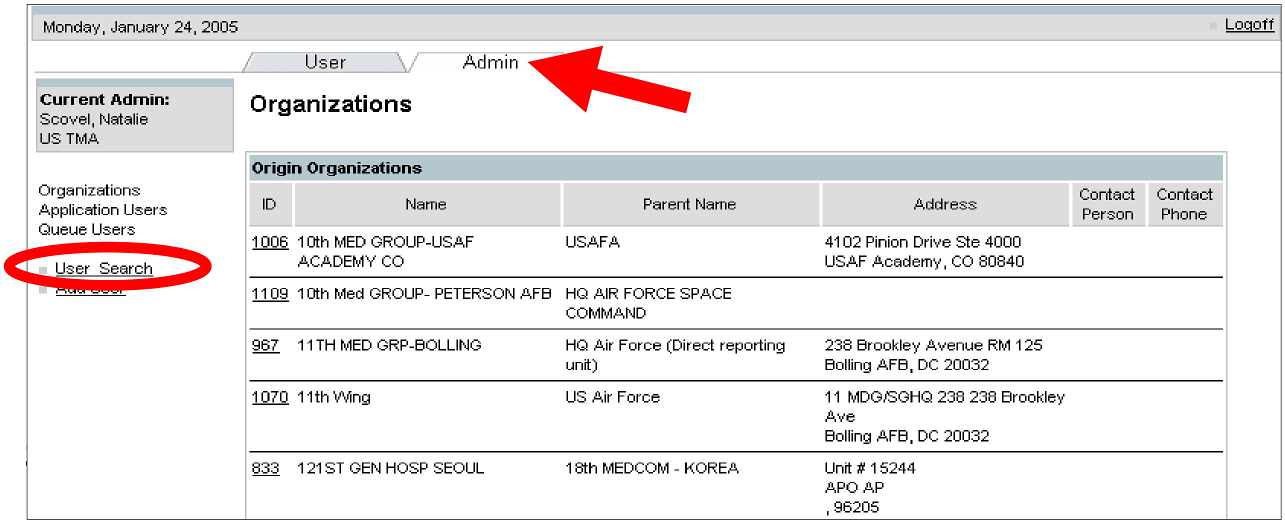
A transfer from one MTF to another can only be executed by the User Admin at the Service level. If a user transfers to a new organization, the User Admin at the receiving location would initiate an action for the transfer according to Service requirements. If a user transfers from one

Service to another; please contact the HIPAA Support Center at: Hipaasupport@tma.osd.mil. The User Admin can only search for users within their level of the hierarchy.

To transfer a user:

1. Select the Admin Tab.

2. Select the User Search hyperlink.

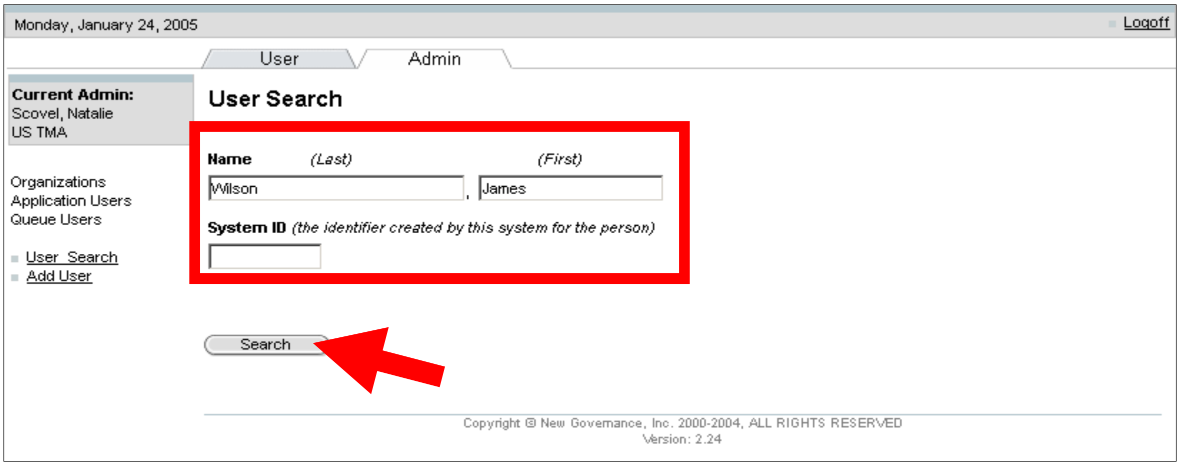


Organizations

Origin Organizations

ID	Name	Parent Name	Address	Contact Person	Contact Phone
1006	10th MED GROUP-USAF ACADEMY CO	USAFA	4102 Pinion Drive Ste 4000 USAF Academy, CO 80840		
1109	10th Med GROUP- PETERSON AFB	HQ AIR FORCE SPACE COMMAND			
967	11TH MED GRP-BOLLING	HQ Air Force (Direct reporting unit)	238 Brookley Avenue RM 125 Bolling AFB, DC 20032		
1070	11th Wing	US Air Force	11 MDG/SGHQ 238 238 Brookley Ave Bolling AFB, DC 20032		
833	121ST GEN HOSP SEOUL	18th MEDCOM - KOREA	Unit # 15244 APO AP , 96205		

3. Click on the Search button.



User Search

Name (Last) (First)

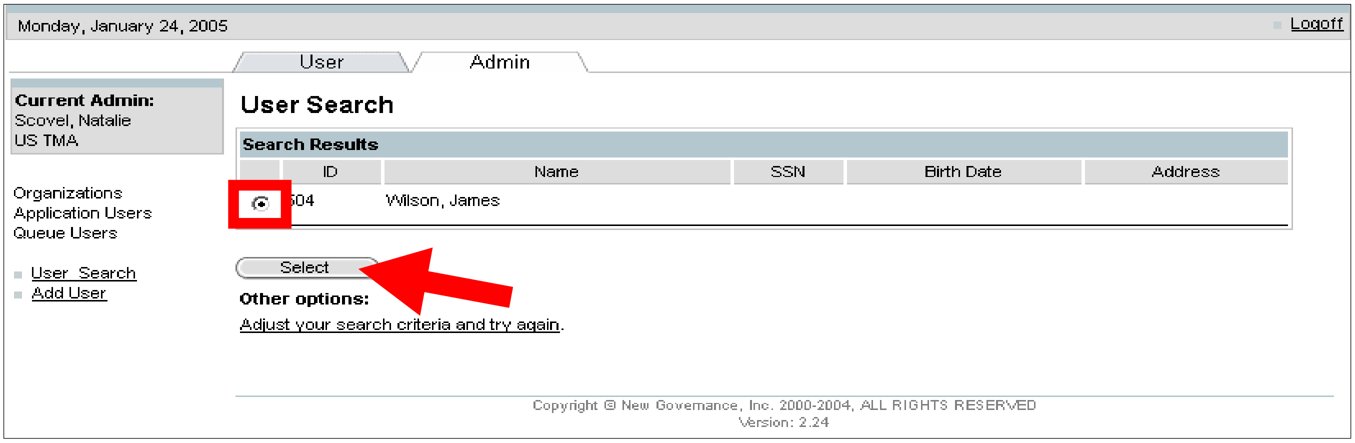
Wilson , James

System ID (the identifier created by this system for the person)

Copyright © New Governance, Inc. 2000-2004, ALL RIGHTS RESERVED
Version: 2.24

4. Click on the radio button for the user to be transferred.

5. Click on the Select button.



Monday, January 24, 2005

Current Admin:
Scovel, Natalie
US TMA

User Search

Search Results

	ID	Name	SSN	Birth Date	Address
●	504	Wilson, James			

Other options:
Adjust your search criteria and try again.

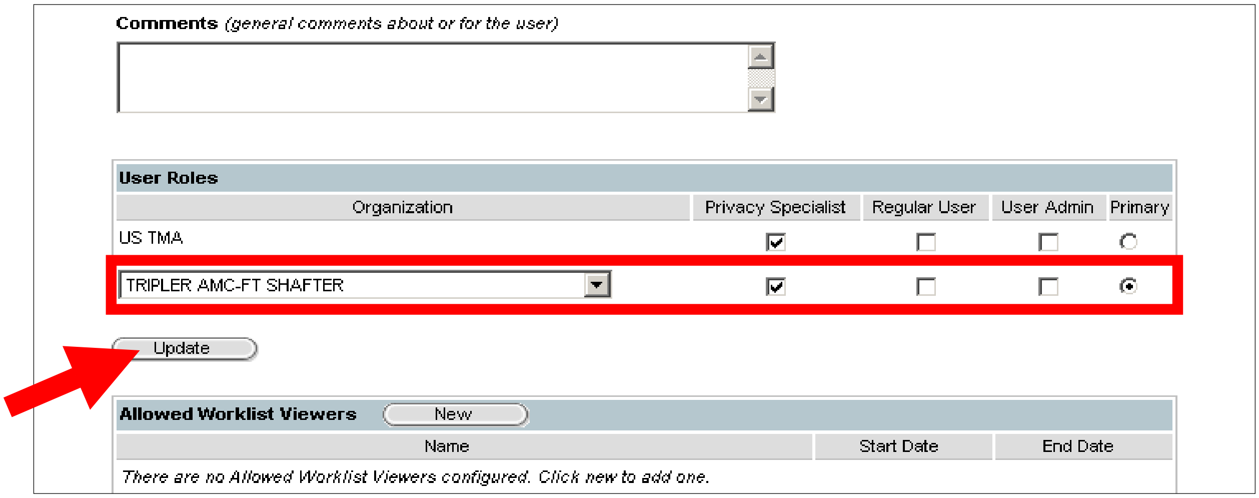
Copyright © New Governance, Inc. 2000-2004, ALL RIGHTS RESERVED
Version: 2.24

6. Scroll down to the User Roles section.

7. Select the new organization from the drop-down box and make any changes to the user role.

8. Select the primary radio button for the new organization.

9. Click on the Update button.



Comments *(general comments about or for the user)*

User Roles

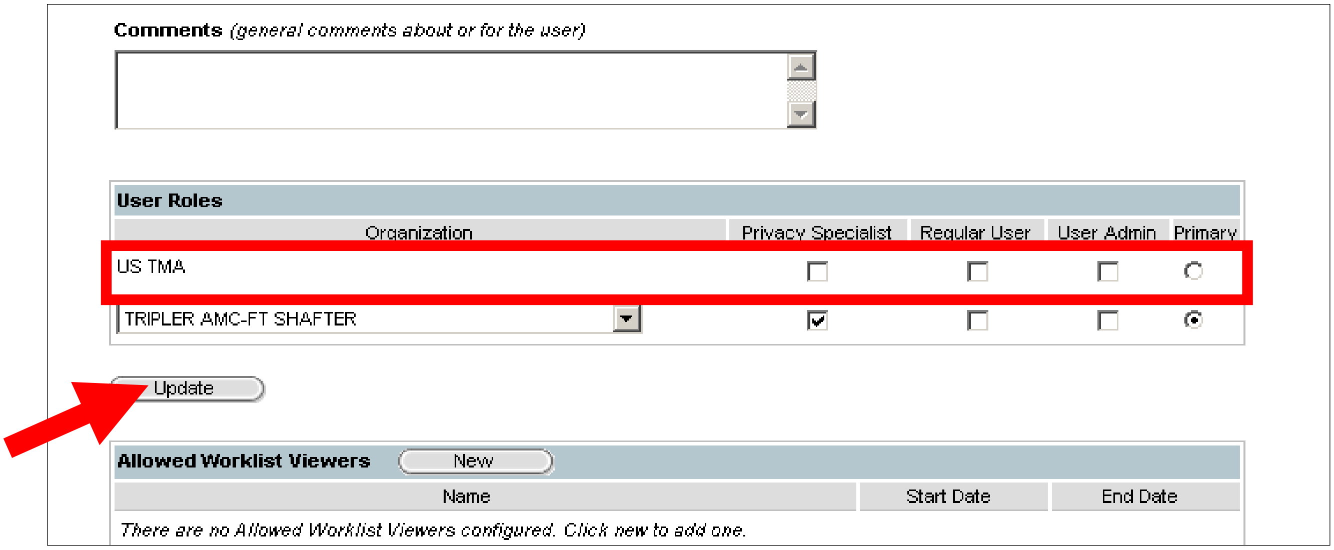
Organization	Privacy Specialist	Regular User	User Admin	Primary
US TMA	☑	□	□	○
TRIPLER AMC-FT SHAFTER	☑	□	□	●

Allowed Worklist Viewers

Name	Start Date	End Date
There are no Allowed Worklist Viewers configured. Click new to add one.		

10. Remove the check for the old organization and role.

11. Click on the Update button.



Comments *(general comments about or for the user)*

User Roles

Organization	Privacy Specialist	Regular User	User Admin	Primary
US TMA	□	□	□	○
TRIPLER AMC-FT SHAFTER	☑	□	□	●

Allowed Worklist Viewers

Name	Start Date	End Date
There are no Allowed Worklist Viewers configured. Click new to add one.		

7.0 USER ADMIN GLOSSARY

Add Organizations: Add Organizations is a hyperlink on the Admin Tab that allows the User Admin to enter new user facilities to the current listing.

Add User: Add User in a hyperlink on the Admin tab that allows the User Admin to enter a new user into the PHIMT database.

Admin Tab: The Admin tab is one of two label tags that provide access to a set of user admin activities that regulate administrative functions of the PHIMT database. These activities include: maintaining disclosure types and organizations, and creating/modifying users.

All User's List: All User's List is a hyperlink on the Admin tab that provides a listing of all users in the PHIMT database. This hyperlink makes user management available.

Back: Back is a navigation button that allows the user to go back to the previous screen.

Logoff: Logoff is a hyperlink that allows the user to exit PHIMT and return to the login screen.

Login: Login is PHIMT's Opening screen that requires a User ID and password for entry.

My Profile: My Profile is a hyperlink on the User tab that allows users to update their personal information and create user-to-user relationships.

My Requests: My Requests is a hyperlink on the User tab that allows users to view the status of all requests initiated by them.

MTF: MTF is the PHIMT acronym for Military Treatment Facility.

My Worklist: My Worklist is a hyperlink on the User tab that allows users to view and process all requests that are currently tasked to them. This hyperlink serves as an electronic inbox by allowing you to perform "desk duties."

Next: Next is a navigation button that allows the user to proceed to the next step.

New: New is an action button that allows the user to develop a new item (patient, organization) in PHIMT.

Organization: In PHIMT, an organization is a logical or physical entity such as MTF, a service, or TMA.

Organization Management: Organization management is a hyperlink on the Admin tab that allows the User Admin to create and/or modify facilities within the PHIMT database. This PHIMT user term refers to the process of maintaining a user's organization profile and status.

PHI: PHI is an acronym for Protected Health Information.

PHIMT: PHIMT is an acronym for Protected Health Information Management Tool. This application tracks disclosures of legally guarded health information with regards to HIPAA compliance.

Requester: Requester is a PHIMT term that refers to the individual or agency asking for the disclosure.

Role: In PHIMT, role refers to a named collection of permissions. A role allows users with the same permissions to be grouped under a unique name such as: Regular User, User Admin, or Privacy Specialist.

Save: Save is a PHIMT action button that allows users to keep data entries and information.

Search: Search is a PHIMT action button that allows users to look for a particular patient or activity.

Select: Select is a PHIMT action button that allows users to choose a particular patient or activity.

Status Box: The status box is a gray block in the upper left corner of all PHIMT screens that displays the current information for user admin, patient, or activity; depending on actions being performed.

Switch Organizations: Switch organizations is a hyperlink on the User tab, that allows users who are assigned to more than one facility to change primary status between those facilities.

TMA: TMA is an acronym for Tricare Management Activity.

Update: Update is a PHIMT action button that allows users to update information or perform additional activities.

User Admin: User Admin is a PHIMT role that allows the user to set up all accounts for users within their facilities as directed by the Military Treatment Facility (MTF) Privacy Officer. The User Admin creates and assigns User Names and Passwords, adds/modifies Users from within their Service, assigns roles, creates user to user relationships, verifies the identity of individuals who access PHIMT, and provides login information to users. The User Admin also creates workflows by routing the requests of a Regular User to a Privacy Specialist and from a Privacy Specialist to another Privacy Specialist, if necessary.

User Profile: User Profile is a PHIMT term that is used when referring to the Add User activity. This profile screen allows the user admin to enter personal information and preference data about a new user.

User Role: User role is a PHIMT term that refers to a named collection of permissions. Each role has varying degrees of permissions. Roles allow users with the same permissions to be grouped under a unique name (ex. Regular User, User Admin, and Privacy Specialist.) The MTF Privacy Officer usually determines the appropriate roles.

User Search: User Search is a hyperlink on the Admin tab that allows the user admin to search for a particular user.

User Tab: The User Tab is one of two label tags that provide access to all PHIMT user related information. This information includes: profile, requests, worklist, and organizational switches. This tab is designed to track all tasks that are assigned to the User.

User-to-User Relationship: User-to-User Relationship is a PHIMT term that refers to the different user types and how they work with one another. The User Admin creates this relationship as directed by the MTF Privacy Officer. The Privacy Officer understands how the MTF manages disclosures. The User Admin understands how to create a workflow by routing requests of a Regular User to a Privacy Specialist and from a Privacy Specialist to another Privacy Specialist, thereby creating the working relationships between the different PHIMT users. Multiple user relationships can be established throughout the Facility.

8.0 USER ADMIN ROLE PERMISSIONS

PHIMT USER ADMIN PERMISSIONS	
PHIMT User Admin Tab	**Enabled Permissions**
Logon/Logoff	Both
User Tab	Change password Switch to other organizations Update address User profile User workflow User worklist Workflow request
Admin Tab	All users list Attach file Organization management User management
Patient Tab	None (can perform patient profile and patient relationship activities.)
Requests Tab	None (perform new request: route to my worklist activity.)
Requester Tab	None

This document contains proprietary information and will be handled within Government regulations. It is intended solely for the use and information of the Military Health System.